



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

August 7, 2008

Information Systems Management Report

David Litchliter, Executive Director
Mississippi Department of Information Technology Services
301 North Lamar Street
Suite 508
Jackson, Mississippi 39201-1495

Dear Mr. Litchliter:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls and selected MVS operating system controls of the Mississippi Department of Information Technology Services as of June 30, 2008. 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 March 12, 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 Information Technology Services' 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, testing, and discussions with Mississippi Department of Information Technology Services.

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. We consider the deficiency noted in Finding Number One (1) to be a significant deficiency in 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 Information Technology 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.

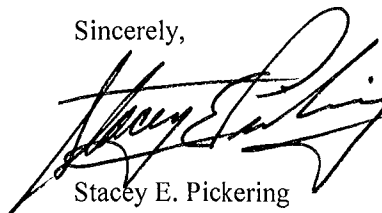
Please review the recommendations included in this report and submit a plan to implement them by August 28, 2008. The enclosed findings contain more information about our recommendations.

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 Information Technology Services throughout this assessment. If you have any questions or need more information, please contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Stacey E. Pickering", written over a white background.

Stacey E. Pickering
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 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
A. <u>SIGNIFICANT DEFICIENCY IN INTERNAL CONTROL</u>	
Finding 1. The Use of Non-standard MVS Security Settings Should Be Reviewed and Limited...	6
B. <u>IMMATERIAL WEAKENSSES IN INTERNAL CONTROL</u>	
Finding 2. ITS Should Insure All Federal MVS Audit Findings Are Evaluated and Documented..	7
Finding 3. ITS Should Set Expiration Parameters for All Individual's RACF Passwords.....	7
Finding 4. ITS Should Reduce Update and Alter Access to Key MVS Libraries.....	8
Finding 5. ITS Should Designate an Information Security Officer and Information Security Program	8

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 30, 2008**

I. ABBREVIATIONS USED IN THIS REPORT

IPL	MVS Initial Program Load (start-up)
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
MVS	Multiple Virtual Storage – IBM Operating System
OSA	Office of the State Auditor
RACF	Resource Access Control Facility (IBM)

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 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 Information Technology Services (ITS) to support the integrity and security of the financial information processed by the computer systems of the State of Mississippi by its Agencies using MVS operating systems on IBM z/OS mainframes managed by ITS at its computing center in Jackson, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA):

- Met with ITS IS management and the OSA financial auditors to gain an understanding of the critical ITS processes and controls;
- Interviewed selected ITS 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) 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.

IBM z/OS MVS security settings best practices standards are available in IBM Redbooks.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 30, 2008**

IV. FINDINGS AND RECOMMENDATIONS

SIGNIFICANT DEFICIENCY IN INTERNAL CONTROL

1. The Use of Non-standard MVS Security Settings Should Be Reviewed and Limited

Finding:

Our review indicated that ITS had one set of MVS system parameters which did not comply with industry standard security parameters. Although this configuration was the result of an intentional configuration choice for multi-agency computer system accounting and segregation purposes, the resulting unintentional effect on security could be detrimental.

MVS security standards for systems involved with sharing of information with Federal Tax information systems are defined in the Internal Revenue Manual Part 10, Chapter 8.

Failure to utilize the security systems provided in MVS could lead to inappropriate access of computing equipment.

Recommendation:

We recommend that ITS review the MVS operating systems security configuration to ensure that MVS configuration choices compliment other security system features, as outlined in the Internal Revenue Manual Part 10, Chapter 8.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 30, 2008**

IMMATERIAL WEAKENSSES IN INTERNAL CONTROL

2. ITS Should Insure All Federal MVS Audit Findings Are Evaluated and Documented

Finding:

During the last two years the IBM MVS operating system security was reviewed by consultants engaged by Federal agencies which share taxpayer information with Mississippi state agencies. In the Federal review process, MVS security configuration findings and recommendations were issued by the Federal agencies. ITS resolved many of the findings, but a number of the Federal findings still appear to be unresolved, and are not documented as to the reasons why the exception conditions noted should exist. In some cases the Federal recommendations may not be feasible for ITS to implement, or other conditions may exist that would make the recommendations possibly not relevant.

Failure to resolve all findings or to document why exceptions to the Federal findings that still exist, or where the resolution of the findings as suggested by the Federal audit teams is not either feasible or appropriate in the ITS environment, could result in complications for sharing of Federal information.

Recommendation:

We recommend that all remediation of Federal information security audits be fully addressed and documented as to the changes made, and if areas where differences of opinion or conditions do not allow such suggested changes, the reasons supporting the ITS position should also be documented. An open items issue control tracking document should be compiled to assure that all findings of Federal security audits are timely and fully addressed.

3. ITS Should Set Expiration Parameters for All Individual's RACF Passwords

Finding:

Our review of RACF security settings located five user-id's in ITS with passwords set to never expire. Generally non-expiring passwords should be reserved only to system tasks which could require continuous service. Otherwise all passwords should be set to expire with in policy days.

This criteria for best practices in password expiration as established by Mississippi Department of Information Technology Services in the State of Mississippi Enterprise Security Policy, and is an industry standard security best practice.

Recommendation:

We recommend that all passwords for individual user-ids should be set to expire within State policy of no more than every six months.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES
AS OF JUNE 30, 2008**

4. ITS Should Reduce “Update and Alter” Access to Key MVS Libraries

Finding:

Our review (and Federal reviews) noted that there appears to be excessive personnel which have update and alter capabilities to key MVS libraries.

The access to key MVS libraries differs by each library but in each case the number of personnel with update or alter access could be reduced. Reducing the number of personnel that can change these libraries will assist in compliance with Federal reviews and reduce any unnecessary exposures to MVS security.

Recommendation:

We recommend that update and alter capabilities to key MVS libraries should be limited to only a core group of key MVS systems programmers. ITS should review access authority to MVS key libraries on regular basis to ensure that access granted is still appropriate.

5. ITS Should Designate an Information Security Officer and Information Security Program

Finding:

The State of Mississippi Enterprise Security Policy was created to provide a data security policy framework. At the time of our review, the policy’s effectiveness appeared limited, as ITS did not have any individual designated as the agency’s Information Security Officer, nor did it have a formalized security program. Security duties were shared among various technical staff members, leading to possible incomplete coverage and conflict of duties.

Recent audit findings reinforce the need for an independent security administration in ITS. We also note that The State Of Mississippi Enterprise Security Policy has not been updated to include issues such as Federal Tax information sharing, HIPPA and other compliance topics not considered in the current policy. All state agencies are basically in need of information security guidance and considering the fact that directly or indirectly they are a component on the ITS network, the fostering of a strong State information security program should belong with ITS.

Recommendation:

We recommend that ITS designate an Information Security Officer, and create an Information Security Plan which supports the goals of the State of Mississippi Enterprise Security Policy. We note that ITS management and staff have also recognized the need for an Information Security Officer. This is supported under CobiT control objective DS5 “Ensure Systems Security” which contains process goals by focusing on defining IT security policies, procedures and standards, including monitoring, detecting, and resolving security vulnerabilities and incidents. A strategic goal for an information security program should include a complete and current Mississippi Enterprise Security Policy that serves a security focal point for security guidance for all state agencies.

End of Report