



State of Mississippi

OFFICE OF THE STATE AUDITOR
PHIL BRYANT
AUDITOR

February 1, 2002

Financial Audit Management Report

Ed Buelow, Jr., Chairman
Mississippi State Tax Commission
1577 Springridge Road
Raymond, Mississippi 39154

Dear Mr. Buelow:

Enclosed for your review are the financial audit findings for the Mississippi State Tax Commission for the Fiscal Year 2001. In these findings, the Auditor's Office recommends the Mississippi State Tax Commission:

1. Strengthen access controls over the AS400 computer system;
2. Strengthen controls over user accounts for the Novell and UNIX systems;
3. Strengthen controls over physical security of the computer room;
4. Strengthen Resource Access Control Facility (RACF) access user settings; and
5. Implement employee termination procedures.

Please review the recommendations and submit a plan to implement them by February 25, 2002. 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 is not intended to be and should not be used by anyone other than these specified parties.

Mississippi State Tax Commission
February 1, 2002
Page 2

I hope you find our recommendations enable the Mississippi State Tax Commission to carry out its mission more efficiently. I appreciate the cooperation and courtesy extended by the officials and employees of the Mississippi State Tax Commission throughout the audit. If you have any questions or need more information, please contact me.

Sincerely,

Phil Bryant
State Auditor

Enclosures

The Office of the State Auditor has completed its audit of selected accounts included on the financial statements of the Mississippi State Tax Commission for the year ended June 30, 2001. These financial statements are consolidated into the State of Mississippi's Comprehensive Annual Financial Report. The Office of the State Auditor's staff members participating in this engagement included Rob Robertson, Karlanne Coates, CPA, Wendi Goodwin, Judy Bounds, Daphonie Moulder, Shane Atkison, Eleace Sawyers, Geeta Sethi, and Mike Sumrall, CISA.

The fieldwork for audit procedures and tests was completed on October 31, 2001. These procedures and tests 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 and tests of transactions for this or other fiscal years to ensure compliance with legal requirements.

Internal Control over Financial Reporting

In planning and performing our audit of selected accounts included on the financial statements, we considered the Mississippi State Tax Commission's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on these accounts and not to provide assurance on the internal control over financial reporting.

However, we noted certain matters involving the internal control over financial reporting and its operation that we consider to be reportable conditions. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control over financial reporting that, in our judgement, could adversely affect the department's ability to record, process, summarize and report financial data consistent with assertions of management in the financial statements. These matters are noted under the heading **REPORTABLE CONDITIONS**.

A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are considered to be material weaknesses. However, we believe none of the reportable conditions described in this letter is a material weakness.

In addition, we noted other matters involving the internal control over financial reporting that require the attention of management. These matters are noted under the heading **IMMATERIAL WEAKNESSES IN INTERNAL CONTROL**.

Compliance

As part of obtaining reasonable assurance about whether selected accounts included on the financial statements of the Mississippi State Tax Commission are free of material misstatement, we performed tests of compliance with certain provisions of laws, regulations, contracts and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. We are pleased to report the results of our tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.

REPORTABLE CONDITIONS

Access Controls over the AS400 Computer System Should Be Strengthened

Finding:

During our review of the AS400 computer system at the Mississippi State Tax Commission - Division of Alcohol Beverage Control for fiscal year 2001, we noted the following weaknesses:

- Two vendor-supplied user profiles had the original password provided by the vendor. One of the profiles had expired and had to be changed before the profile could be used. All passwords should be established by agency personnel.
- Seventeen users had security officer rights. This appears to be an excessive number.
- Several users had not signed onto the system in over six months, and several passwords had not been changed in over a year. This appears to indicate these employees had no need for access to the computer system. Passwords should be changed at set intervals to protect the user's access security.
- An inactive job timeout period was not set. This could allow unauthorized access to a terminal left unattended for a long period of time.

Control Objectives for Information and Related Technology (CobiT) guidelines, as well as recognized industry best practices, require adequate access controls. Failure to provide access controls could allow unauthorized access or fraud to occur without being detected.

Recommendation:

We recommend the Mississippi State Tax Commission - Division of Alcohol Beverage Controls implement the following changes in the security settings for the AS400 computer system:

- All vendor-supplied user profile passwords should be established by agency personnel.
- The agency should review all users with security officer rights and ensure those rights are needed. If these rights are needed, application level controls should be reviewed for appropriate access levels.

- The user listing should be reviewed monthly to identify inactive accounts. Any accounts inactive for 90 days should be disabled.
- An inactive job timeout period should be established to prevent unauthorized access should a terminal be left unattended for long periods of time.

Access Controls Over User Accounts Should Be Strengthened for the Novell and UNIX Systems

Finding:

During our review of the Novell and UNIX system settings at the Mississippi State Tax Commission for fiscal year 2001, we noted the following weaknesses:

- Novell system user ADMIN did not require a unique password, and an expiration date was not set.
- Several Novell system user accounts did not require passwords or unique passwords.
- Several Novell system user accounts did not have an expiration date. We also noted that UNIX system passwords were not set to expire.
- The UNIX system did not have password aging which would help ensure security of employee passwords.
- UNIX system users had Write permissions to some program files. This could allow the users to alter program files.

Controls Objectives for Information and Related Technology (CobiT) guidelines, as well as recognized industry best practices, require adequate access controls. Failure to provide access controls could allow unauthorized access or fraud to occur without being detected.

Recommendation:

We recommend the Mississippi State Tax Commission strengthen controls over user accounts for the Novell and UNIX systems by performing the following:

- The Novell system user ADMIN should require a unique password and have a set expiration date.
- The agency should implement rules for passwords that address expiration dates and password aging limits. All Novell system users should require a unique password and have an established password change interval.
- Clear policies should be written governing user access rights. The agency should review all UNIX system users with Write permission to ensure program security is not compromised.

IMMATERIAL WEAKNESSES IN INTERNAL CONTROL

Controls Over Physical Security of the Computer Room Should Be Strengthened

Finding:

During our review of computer room security at the Mississippi State Tax Commission - Division of Alcohol Beverage Control for fiscal year 2001, we noted the fire extinguisher had an inspection date of December 1998. We also noted the computer room did not have any type of emergency lighting.

Control Objectives for Information and Related Technology (CobiT) guidelines, as well as recognized industry best practices, require adequate physical controls over the computer system. This includes protection against fire or power failure to ensure limited disruption during an emergency situation.

Recommendation:

We recommend the Mississippi State Tax Commission - Division of Alcohol Beverage Control strengthen physical security controls over the computer room by ensuring fire extinguishers have a current inspection. We further recommend that the agency provide a system of emergency lighting to minimize disruption during a power failure.

Resource Access Control Facility (RACF) Access User Settings Should Be Strengthened

Finding:

During our review of the Mississippi State Tax Commission for fiscal year 2001, we noted several weaknesses in the Resource Access Control Facility (RACF) user settings for the State Tax Commission headquarters, as well as the Division of Alcohol Beverage Control. Weaknesses noted were:

- The password change interval was not consistent. Some accounts were set to not applicable, and others were set to 30 or 60 days. Management should establish a consistent interval for changing passwords which applies to all users.
- Several RACF user accounts had been inactive for a year or longer. Inactive user accounts should be disabled.

Control Objectives for Information and Related Technology (CobiT) guidelines, as well as recognized industry best practices, require adequate access controls. Failure to provide access controls could allow unauthorized access or fraud to occur without being detected.

Recommendation:

We recommend the Mississippi State Tax Commission strengthen controls over Resource Access Control Facility (RACF) user settings at both the headquarters and the Division of Alcohol Beverage Control. The agency should establish and enforce adequate password expiration intervals for all RACF user accounts. Also, inactive RACF user accounts should be disabled to prevent unauthorized access.

Employee Termination Procedures Should Be Implemented

Finding:

During our review of the Mississippi State Tax Commission, we noted two terminated employees had active user accounts. *Control Objectives for Information and Related Technology (CobiT)* guidelines, as well as recognized industry best practices, require existence of adequate termination procedures to terminate system access to former employees. Failure to provide termination procedures could allow unauthorized access or fraud to occur without being detected.

Recommendation:

We recommend the Mississippi State Tax Commission implement procedures to ensure the user access of retired or terminated employees is disabled immediately.