STATE OF MISSISSIPPI

OFFICE OF THE STATE AUDITOR
STACEY E. PICKERING
STATE AUDITOR

March 3, 2014

Information Systems Management Report

H. Carey Webb, State Aid Engineer
Mississippi Department of Transportation
Office of State Aid Road Construction
P.O. Box 1850
Jackson, Mississippi 39215-1850

Dear Mr. Webb:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls and selected application controls of the Office of State Aid Road Construction (OSARC). This assessment focused on the adequacy of the OSARC information technology general controls (ITGC) which help to protect the integrity and security of its computer systems and was performed in conjunction with the audit of the State of Mississippi.

The following members of the Office of the State Auditor participated in this engagement: David Ashley, MBA, ME, CISA, CISM, CBCP, CRISC (IS Audit Director) and Mike Ferguson, CISA (IS Audit Manager).

Scope of Our Review

To support our general controls assessment, our procedures were performed through observations and discussions of the information technology general controls (ITGC) of the Office of State Aid Road Construction's Information Systems. The scope of our Information Systems review included information processing technology risks in the following categories: integrity, reliability, availability and access, managing problems and incidents.

Limitations

In planning and performing our limited assessment of the Office of State Aid Road Construction's information systems, we considered the Office of State Aid Road Construction's information technology general controls (ITGC) in order to determine our assessment procedures; however, this review was not for the purpose of expressing an opinion on the effectiveness of the internal control over information systems. Also, 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.

Internal Controls Over Information Systems

As stated previously, our review was intended to be in support of the federal audit of the Office of State Aid Road Construction. Therefore, any exceptions in ITGC are ultimately evaluated as to their impact on federal reporting by the entity.

A deficiency in internal control 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 and correct misstatements on a timely basis. A material weakness is a deficiency or combination of deficiencies in internal control such that there is a reasonable possibility, that a material misstatement of the entity's financial

statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Our consideration of the internal controls over IS was for the limited purpose described in the fourth paragraph and was not designed to identify all deficiencies in internal control over information systems that might be material weaknesses or significant deficiencies and therefore material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our review we did not identify any deficiencies in internal control that we consider to be material weaknesses.

Compliance

As part of obtaining reasonable assurance about whether selected IS general controls of the Office of State Aid Road Construction are functioning as designed, we performed assessments of compliance with industry best practices. However, providing an opinion on compliance with these practices was not an objective of our assessment and accordingly, we do not express such an opinion.

Summary

We identified deficiencies involving internal control over ITGC that we consider to be significant deficiencies in internal control over IS. In addition, three control deficiencies were also noted. These matters are noted under the headings SIGNIFICANT DEFICIENCIES and CONTROL DEFICIENCIES. Please review the recommendations included in this report and submit a plan to implement them by March 28, 2014. The enclosed findings contain more information about our recommendations. During future engagements, we may review the findings in this engagement report to ensure that procedures have been initiated to address this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our general controls assessment of the Office of State Aid Road Construction's Information Systems and the results of that assessment. Accordingly, this communication is not suitable for any other purpose. However, this report is a matter of public record and its distribution is not limited.

We appreciate the cooperation and courtesy extended by the officials and employees of the Office of State Aid Road Construction throughout this review. If you have any questions or need more information, please contact me.

Sincerely,

Patrick Dendy, CPA
Director, Department of Audit

Enclosures

OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
OFFICE OF STATE AID ROAD CONSTRUCTION
AS OF FEBRUARY 13, 2014

TABLE OF CONTENTS

Page No.

I. ABBREVIATIONS USED IN THIS REPORT 4

II. REVIEW OBJECTIVES AND APPROACH 5

III. STANDARDS FOR BEST PRACTICES 5

IV. FINDINGS AND RECOMMENDATIONS 6

SIGNIFICANT DEFICIENCIES

Finding 1. OSARC Should Implement a Program of IT Governance 6

Finding 2. OSARC Should Implement a Formal Information Security Policy 7

Finding 3. OSARC Should Comply with Guidelines for Offsite Tape Storage 7

CONTROL DEFICIENCIES

Finding 4. OSARC Should Implement a Formal Change Management Process 8

Finding 5. OSARC Should Adhere to Policy on Password Expiration 8

Finding 6. OSARC Should Establish a Formal Disaster Recovery Process 9

OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
OFFICE OF STATE AID ROAD CONSTRUCTION
AS OF FEBRUARY 13, 2014

I. ABBREVIATIONS USED IN THIS REPORT

IS	Information Systems
IT	Information Technology
ITGC	Information Technology General Controls
ITS	Mississippi Department of Information Technology Services
MIS	Management Information Systems
OSA	Office of the State Auditor
OSARC	Office of State Aid Road Construction

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 Office of State Aid Road Construction to support the integrity and security of the information processed by the computer systems of the Office of State Aid Road Construction 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 Office of State Aid Road Construction management and the OSA auditors to gain an understanding of the critical Office of State Aid Road Construction processes and controls;
- Interviewed selected Office of State Aid Road Construction technology personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- 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. STANDARDS FOR 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 utilize 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.

Additional sources for Information Systems control criteria include *The State of Mississippi Department of Information Technology Services' Enterprise Security Policy* and the U. S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM). This manual provides guidance for reviewing information system controls affecting integrity, confidentiality, and availability of computerized data. See http://www.gao.gov/products/GAO-09-232G.

IV. FINDINGS AND RECOMMENDATIONS

SIGNFICANT DEFICIENCIES

1. OSARC Should Implement a Formal Program of IT Governance.

Finding:

Information Technology (IT) governance is the leadership and organizational structures and processes that ensure an organization's IT investments sustain and extend business strategies and objectives. IT governance decision-making frameworks and processes help define how all IT investment decisions will be made, where accountability lies for those decisions and the ongoing management of IT investments and technology standards.

During our review of information systems controls at the Mississippi Department of Transportation Office of State Aid Road Construction we noted that the agency had not established a formal program of IT Governance. The lack of a written program of IT Governance and its effective implementation may cause issues with project overruns and poor values to cost measures. In addition, without supporting policies, actions become difficult to defend in situations such as employee discipline and regulatory compliance.

CobiT PO6.4 calls for organizations to "Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly."

The *Mississippi ITS Enterprise Security Policy,* Part I, Chapter 1, Rule 1.11F states, "Each Agency must develop, implement, and maintain their individual agency IT security policy. Each agency will annually review and revise (as needed) its security policy."

Policies, procedures, and standards define IT organizational behavior and uses of technology. They are a part of the written record that defines how the IT organization performs services that support the organization. IT policies typically cover topics such as security processes, risk management, roles and responsibilities, development practices, operational practices, incident management, project management and vulnerability management.

Recommendation:

We recommend that OSARC establish IT governance through an IT steering committee that will be responsible for setting long-term IT strategy and ensure that IT processes will effectively meet the agency's business needs. Additionally, we recommend OSARC implement a program of IT governance that will address change management, quality management, security management, performance optimization and establish an effective organizational structure and clear statements of roles and responsibilities.

This governance program should include formal policies and procedures. While ITS policies can certainly be used as a guideline for agency policies and procedures, each agency must have its individual policies and procedures as stated above. Policies should be general enough in nature to serve as guidelines for the area to be covered yet specific enough to cover the areas of governance for the agency where guidance might be needed. In addition, these polices should be reviewed and changed accordingly on at least an annual basis or more frequently if business process changes dictate a need to do so. Management should approve all policies and procedures, as well as changes to these

documents. In addition, a system that is appropriate to organizational culture should be developed to disseminate policies and procedures and any related changes to applicable parties in a timely manner.

2. OSARC Should Implement a Formal Information Security Policy.

Finding:

During our review of information system controls at the Mississippi Department of Transportation Office of State Aid Road Construction we noted the agency has not adopted a formal Information Security Policy or Enterprise Security Plan.

During 2009, the *Mississippi ITS Enterprise Security Policy* was substantially updated and strengthened and requires all state agencies to have a written information security plan, conduct a security risk analysis, implement a data classification scheme, and provide for periodic external security reviews.

The lack of a formal Information Security Policy can lead to a breakdown of basic security practices in the area of application security, LAN/WAN security, management of the security application, and Internet protocol.

Recommendation:

Practices outlined in the *Mississippi ITS Enterprise Security Policy* are typical of appropriate standards for any moderate sized IT organization. While full compliance with all facets of the policy may be an economic challenge for OSARC, beginning steps to become compliant with the policy are necessary. We recommend that OSARC create a plan of compliance with industry standards and State policy to ensure progress towards a more robust documented information security plan.

3. OSARC Should Comply with Guidelines for Offsite Tape Storage.

Finding:

Part 1, Chapter 12, Rule 12.4B of the *Mississippi ITS Enterprise Security Policy* states, "Backup and recovery materials (tapes, manuals, etc.) must be kept at a site that meets all security measures defined in this document. This site should be accessible 24/7/365."

In our review of information systems controls at the Mississippi Department of Transportation Office of State Aid Road Construction, we noted although the agency does take backups offsite, they do not follow ITS policy or business best practices in doing so. During the audit process, we were informed that the backup tapes were taken home each night by IT personnel. Such practices could lead to loss of sensitive data or failure to recover computerized operations in a timely manner. As specified above, the backup media should be stored in a location that meets security measures such as restricted physical access, environmental controls (i.e., temperature, moisture, etc.), fire suppression, etc. In addition, these tapes should be available for use 24 hours per day.

Recommendation:

We recommend that Mississippi Department of Transportation Office of State Aid Road Construction follow guidelines of the *Mississippi ITS Enterprise Security Policy* and store backup media in offsite facilities that meet such guidelines. In addition, we recommended that storage of backup media be

handled by government entities such as the Mississippi Department of Archives and History or private entities with facilities to handle such media. It is further recommended that a rotation of offsite backups be maintained taking into account the need to use backup tapes from prior periods such as month end. A log of offsite tapes should be also be maintained.

CONTROL DEFICIENCIES

4. OSARC Should Implement a Formal Change Management Process.

Finding:

Proper controls on program changes are important to maintain assurances that only program changes authorized by management are placed into production. This principle is supported by CobiT AI6 Manage Changes which states, "All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner."

Our review revealed OSARC has no formal change management procedures or processes for important changes to the network and firewall application systems. Although changes are initiated through a network change form, there are no written procedures to manage the changes.

Recommendation:

We recommend that the Mississippi Department of Transportation Office of State Aid Road Construction develop written policies and procedures to govern the change management process for the network and firewall and all application systems. In the evaluation of controls surrounding the application systems, OSARC should also implement best practice program change controls that would include the following practices:

- Document changes in a formal manner.
- Achieve a higher segregation of duties in the programming process.
- Provide for sign-off where appropriate for assignment and completion of program change steps.
- Provide for separate quality assurance from the programmer making the changes.

5. OSARC Should Adhere to Policy on Password Expiration.

Finding:

Part 1, Chapter 11, Rule 11.4E of the *Mississippi ITS Enterprise Security Policy* states, "The password change interval is a maximum of ninety (90) days; however, ITS recommends that agencies consider using a 30 or 60 day interval depending on the classification of their data. Password reuse should be minimized or prohibited."

During our review of information systems controls at the Mississippi Department of Transportation Office of State Aid Road Construction, we noted that the agency does not periodically expire passwords. Non-expiring user passwords prevent password rotation and, can result in the possibility of unauthorized password discovery.

Generally, non-expiring passwords should be reserved only for system tasks which require continuous service.

Recommendation:

We recommend that Mississippi Department of Transportation Office of State Aid Road Construction implement procedures to ensure that password use complies with the *Mississippi ITS Enterprise Security Policy.* Procedures should include expiring passwords on any User ID that does not require a static non-expiring password, such as a computerized processes or system administrators.

6. OSARC Should Establish a Formal Disaster Recovery Process.

Finding:

During our review of the information system controls at the Mississippi Department of Transportation Office of State Aid Road Construction (OSARC), we noted the agency did not have a formal written disaster recovery plan. Without a documented and tested written disaster contingency plan in place, recovery efforts at OSARC could be significantly delayed or even cause failure to recover some information assets in the event of a disruption.

Systems availability is a key control issue for any organization. *Control Objectives for Information and Related Technology (CobiT)*, Sections DS4 through DS10 set standards for the entire contingency planning process.

Recommendation:

We recommend that the Mississippi Department of Transportation Office of State Aid Road Construction develop and implement a formal disaster recovery plan documenting procedures to be followed during an emergency. The disaster recovery plan should be reviewed and tested at least on an annual basis and employees should be made aware of their responsibilities in the event of a disaster. Both the review and test should be documented and any such documentation should be retained for audit purposes.

End of Report