



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

January 25, 2008

**Information Systems Management Report**

Gray Swoope, Executive Director  
Mississippi Development Authority  
P. O. Box 849  
Jackson, MS 39205

Dear Mr. Swoope:

The Office of the State Auditor has completed its limited assessment of the EDP general controls and selected application controls of the Mississippi Development Authority Homeowner Assistance Program as processed by Reznick Mississippi LLC, begun as of June 4, 2007. 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 EDP review engagement included: Toby Frazier, CISA, Mike Ferguson, and LaDonna Johnson.

The fieldwork for these assessment procedures was completed on July 31, 2007. 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 EDP general controls, we considered the Mississippi Development Authority Homeowner Assistance Program'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 Reznick Mississippi LLC personnel and limited testing of information of the eGrants Plus 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. We consider the deficiency noted in Finding Number Ten (# 10) 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 do not believe this significant deficiency identified in this report to be a material weakness.

We also noted 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 EDP general controls of the Mississippi Development Authority's Homeowner Assistance Program 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.

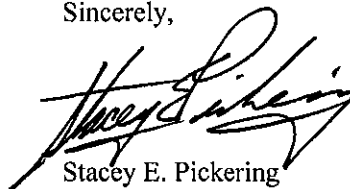
Please review the recommendations included in this report and submit a plan to implement them by February 15, 2008. The enclosed findings contain more information about our recommendations.

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 Development Authority and Reznick Mississippi LLC 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  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

**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 DEFICIENCIES IN INTERNAL CONTROL</u>	
Finding 1. Reznick MS Should Develop a Disaster Contingency Plan.....	6
Finding 2. Reznick MS Should Formalize Information Security Administration.....	6
Finding 3. Reznick MS Should Consolidate Security Administration Duties and Practices.....	7
Finding 4. All System Users Should Have Consistent Password Policies.....	7
Finding 5. Change Control Board Program Change Authorizations Should Be Signed-off.....	8
Finding 6. A Program Version Control Process Should Have Been Implemented to Compliment the CCB Process.....	8
Finding 7. Software Development Quality Control Processes Should Not Be Contractually Waived.....	9
Finding 8. Software Change Task Contracts Should Not Be Written in Arrears of Actual Work Done.....	9
Finding 9. Reznick MS - STR Task Change Order 006 Agreement Should Be Documented.....	10
 <u>SIGNIFICANT DEFICIENCY IN INTERNAL CONTROL</u>	
Finding 10. IT Applications Internal Audit Report, "ITAR", Should Be Complete.....	12

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

**I. ABBREVIATIONS USED IN THIS REPORT**

Advantage	Advantage Industries, Inc., a Maryland company
CCB	Change Control Board
COTS	Commercial off-the-shelf (ready made software)
CVP	Customer Value Partners Corporation, subcontractor to Reznick MS
DBA	Data Base Administrator
EDP	Electronic Data Processing
eGrants	EGrants application software from STR Inc.
HAP	Homeowner Assistance Program
IP	Internet Protocol address
IT	Information Technology
ITAR	Information Technology Audit Report as created by CVP
ITS	Mississippi Department of Information Technology Services
LAN	Local Area Network
MDA	Mississippi Development Authority
MIS	Management Information Systems
OSA	Office of the State Auditor
POP	Post Office Protocol for e-mail
Reznick MS	Reznick Mississippi LLC contactor to Mississippi Development Authority for operations of the Home Owners Homeowner's Assistance Program
RFP	Request for Proposals
SOW	Statement of Work
STR	STR Grants LLC (eGrants software vendor)
W2K3	Microsoft Windows Server 2003

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

**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 Reznick Mississippi for the Mississippi Development Authority Homeowner Assistance Program (MDA/HAP) to support the integrity and security of the financial information processed by the computer systems of the MDA/HAP at its main office in Jackson, Mississippi. To accomplish these objectives, the EDP Audit Section staff of the Office of the State Auditor (OSA) performed the following:

- Met with MDA/HAP management, Reznick Mississippi management, and the OSA financial auditors to gain an understanding of the critical MDA/HAP processes and controls;
- Interviewed selected Reznick Mississippi 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](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  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

IV. FINDINGS AND RECOMMENDATIONS

**IMMATERIAL WEAKNESSES IN INTERNAL CONTROL**

1. Reznick MS Should Develop a Disaster Contingency Plan

*Finding:*

Disasters such as fire and flood can destroy an operations or computer service center and leave its users without computer processing support. Without computer processing, grant administration processing could halt. To reduce this risk, operations and computer service centers should develop disaster recovery plans.

A review was conducted to determine if there was an adequate disaster recovery plan and procedures for Reznick MS and the Rackspace Ltd. hosted services. As a result, the following weaknesses were identified which could compromise the MDA/HAP program's ability to recover critical systems in the event of an emergency either at the Reznick MS operations center or at hosted services at Rackspace Ltd:

1. MDA/HAP Reznick MS did not have a written disaster plan.
2. Local servers at Reznick MS were not backed-up offsite.
3. The Rackspace Ltd. services contract did not provide for definite timelines and services to be provided for restoration in case a disaster strikes their data center.
4. Systems had not been tested for restoration from back-up files.
5. POP e-mail utilized provides no history of e-mail which history could be lost in a disaster situation.

*Recommendation:*

We recommend that Reznick MS conduct a review for disaster contingency risks associated with its operations, and formalize a written disaster recovery plan appropriate to the risks. This plan should include a review of the Rackspace Ltd. contract to identify any risks associated with this service. Additionally, procedures should ensure appropriate offsite back-up of important Reznick MS servers. Also, disaster recovery procedures should be tested periodically to ensure the recoverability of critical systems.

2. Reznick MS Should Formalize Information Security Administration

*Finding:*

We found that Reznick MS systems' security appears to be functional. However, only limited documentation was available as to security settings and permissions granted to users. It appears a "New User Request Form" was available but not used. Security registrations were being requested by supervisor level management to the hardware group via e-mail. At the time of our review Reznick MS only had POP e-mail, that is, no server to save a history of e-mails. This information was recorded in a Help Desk system. However, Reznick MS had been through several changes of help desk systems, and an audit trail of security permissions was not sufficient.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

Without written security approval documentation, validation of security rights assigned is difficult to accomplish. This is supported in CobiT DS5; Ensure Systems Security, DS 5.4 User Account Management, "Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval process outlining the data or system owner granting the access privileges should be included."

*Recommendation:*

We recommend that Reznick MS utilize written request forms to grant or modify information security rights. A formal review process should be conducted periodically to assure that security rights granted are appropriate.

**3. Reznick MS Should Consolidate Security Administration Duties and Practices**

*Finding:*

At the time of our review, base server security was managed by the Reznick MS hardware group. Secondary user level functional application security settings was split from the systems administration function and was administrated by personnel of Advantage, a subcontractor of Reznick MS.

The Advantage personnel also serve in database administration and programming functions as a subcontractor of Reznick MS. Using a second party programming subcontractor to control the functional security of the application system(s) is a conflict of duties that could lead to inappropriate security administration practices. Our request for information of permissions granted to each employee did not provide sufficient information to determine the appropriateness of security permissions. Sufficient documentation of security permissions granted was not maintained.

*Recommendation:*

We recommend that only the Reznick MS staff assigned to systems security be given all systems and applications security administration and authorities.

**4. All System Users Should Have Consistent Password Policies**

*Finding:*

Our review indicated that the inquiry-only users at the Gulf Coast offices, due to system limitations, did not have periodic password rotation requirements. Also, the passwords were set to never expire.

Potential risks are created for disclosure of recipient information by higher risk factors from non-expiration of passwords. *The Mississippi Enterprise Security Policy in section XVII. Passwords; Guidelines, Protection of, Bad examples requires*, "Passwords should be changed at least every 6 months and never reused."

*Recommendation:*

We recommend that Reznick MS review information security practices and improve its method of password management for the Gulf Coast inquiry-only users.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

5. Change Control Board Program Change Authorizations Should Be Signed-off

*Finding:*

In March 2007 Reznick MS initiated a Program Change Control Board (CCB). This committee's purpose is to approve and implement any changes proposed to the systems for MDA/HAP processing. However, the CCB was implemented very late in the applications change process, and had little effect of control for changes on Phase I. The "Truth" system was written prior to the implementation of the CCB, and prior to the CCB in 2007, program change records were significantly limited. This prior inadequate process and documentation created a risk that unauthorized, unintended, or unverified computer program changes could exist, and the application systems may not perform as intended. Even after the CCB was implemented, control documents were still not being formally approved by appropriate sign-off's or other documentation.

Best practices as supported by CobiT AI6; Manage Changes, requires a formal change control process be implemented, and that changes are authorized by stakeholders prior to migration to production.

*Recommendation:*

We recommend that the CCB documentation reflect the complete status of changes and projects to include documentation of sign-off whether by e-mail or signature of completion of steps in the Change Request Form Template as per the second page of the form.

6. A Program Version Control Process Should Have Been Implemented to Compliment the CCB Process.

*Finding:*

In addition to the Change Control Board, controls are required in practices and or version control software to provide assurances that only authorized changes are put into production. Our review indicated that the subcontractors of Reznick MS, which provided both database administration and programming services to the Reznick MS applications, possessed system administrative rights to the production servers.

Good internal controls require that a programming group maintain complete technical records of all program changes. This would include version control records on each program changed, analyst assigned, record of code changed including change records embedded in code comments areas, documentation of formal quality review testing and documentation of the move of the changed program into production.

Best practices would dictate that programs should only be moved into production by a person other than the person who codes the change. Also, administrative rights to the systems should not be given to programmers.

We inquired through Reznick MS to both of the subcontractors to provide us with detailed program change information which would facilitate our conducting a program version control review as part of our normal general IT controls audit. From a conference call request to both subcontractors, each stated to us that they would provide us with this information; however, we did not receive any further communications from either during our field work period. We notified the Reznick MS PMO during our field work portion of our audit of this apparent deficiency in controls.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

Subsequent to our field work, Reznick MS provided OSA with information from each subcontractor stating that a version control system was in effect during our review period. After evaluating the responses, we were still unable to determine the extent of the actual version control practices stated to have existed at the time of our field work. Therefore, we will attempt to re-review this issue during our next planned EDP audit of MDA/HAP.

*Recommendation:*

We recommend that the subcontractor programming group maintain sufficient documentation and access controls in the change process for program modules and databases. This could be facilitated by utilizing a standard version control software package, with limited systems administration rights to programmers and a method to verify authorization and version levels of programs in production. Placing changed modules into production should be controlled by software or a separate group with the appropriate system administration rights.

**7. Software Development Quality Control Processes Should Not Be Contractually Waived**

*Finding:*

Reznick MS subcontracted with a company named STR Grants LLC for various computer programming services. In many of the Task Order subcontracts between Reznick MS and STR Grants LLC beginning around Task Order 010 commencing September 15, 2006, the following clause was included:

*"The standard software development process involves a normal structure imposed on the development of software. The activities related to the process include requirements analysis, specifications, software architecture, coding, testing, and documentation. Because of time constraints associated with the disbursement process, STR has had to eliminate certain of these activities. Therefore, by accepting this statement of work and the final mutually agreed-to version of Attachment A, Reznick is agreeing to the requirements and specifications contained in this SOW that STR will develop against."*

Although this clause may have increased the speed of the development process, it also waived important development controls which could result in software that does not perform as intended or allow a situation that could require future repairs to software improperly developed.

*Recommendation:*

We recommend that Reznick MS follow appropriate software contract best practices for any contracted software enhancements.

**8. Software Change Task Contracts Should Not Be Written in Arrears of Actual Work Done**

*Finding:*

During our review of software change order tasks, we noted that Task Order 009, Modification #3 appears to be a software programming subcontract between Reznick Mississippi LLC and STR Grants LLC dated September 8, 2006, in the amount of \$114,100.00. In this agreement the following statement was noted:

**"Source:** *Over the past six-plus weeks STR has made changes to the Truth Table, the Truth-based*

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

*Application Report, the Closing (Token) Report, the SASS [sic] Report and the Grant Calculation and Approval page based on real-time requests from Doug Taphouse and Brad Anthony. Rather than stopping the process to develop Change Requests associated with these changes to the Specifications that were originally approved in prior task orders, because of the time sensitive nature of the changes, STR made the changes. This Change Order is a compilation of those changes."*

It appears to EDP Audit that in the statement above, changes were made which should have been included either in prior task orders or new orders should have been written. It appears that this contract was written after the fact of actual work done. Although this contract may have been a strategy to streamline the programming process, utilizing such methodology in effect bypasses the controls that have been established by the State of Mississippi for control of IT projects to provide for certain deliverables for the funds expended.

Work done on change orders becomes difficult to account for, as to the funds expended and the results produced, if actually approved on prior contracts, as this contract appears to have become a vehicle for overruns of costs from prior change contracts.

*Recommendation:*

We recommend that MDA review this Task and Modification agreement for proper form as an expense that was appropriate to be paid in this manner. We also recommend that Reznick MS not bundle residual computer programming tasks into a single contract and task for payment purposes.

9. Reznick MS - STR Grants LLC Task Change Order 006 Agreement Should Be Documented

*Finding:*

The EDP Audit Section of OSA requested Reznick MS to provide a listing of all Task Change Orders involving STR LLC. Task number 006 was indicated as "no task 6" in documentation of tasks provided. We researched MDA records and did not find the Task order; however we located two payments for STR Grants LLC Task 6, one in the amount of \$85,315 in the Reznick, MS billings for May 14 – 31, 2006, and a second in the amount of \$52,760 in the Reznick MS, July 2 – 15, 2006 billings. Additionally a 7.5 percent administration fee was added to these billings.

Existing documentation for STR Task 006 makes it difficult to determine the exact programming work done for the MDA/HAP program by Reznick MS and STR Grants. However Task 008 states *"the Reznick Team has re-evaluated the approach originally outlined in Task Order 006 based on time and budget constraints, and has determined the most expeditious manner to accomplish this verification process is outside of eGrants Plus..."* This would appear to indicate that at least some of the work undertaken in Task 006 may not have been of value. In effect, a new application called "TRUTH" to scorecard applicant eligibility was created external to eGrants Plus in Task 008, as apparently a replacement of the work done in Task 006.

The lack of sufficient documentation on this project creates additional difficulties for EDP Audit to determine the program changes made and the efficiency of the process of EDP control of design and programming. It appears from Task 008 documentation that some of the work for Task 006 may have been lost in redesign and reprogrammed.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

*Recommendation:*

We recommend that the original agreement for Task 006 be located and that MDA review this in relationship to amounts that were paid to Reznick MS as to items billed for May and July 2006 to insure that no duplication of payment was made. Additionally documentation should reflect that the work done in Task 008 was not to replace or re-engineer work done in Task 006. We also recommend if any portion of Reznick MS specified payments to STR Grants LLC for Task 006 was not utilized by the MDA/HAP program, that MDA request a refund of charges for any program design and programming which proved not to be a workable solution.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

**SIGNIFICANT DEFICIENCY IN INTERNAL CONTROL**

10. IT Applications Internal Audit Report, "ITAR", Should Be Complete

*Finding:*

An IT audit review was contracted by Reznick MS with the following stated purpose: "To assure that the HAP's IT assets were appropriately and accurately documented and that they provide sufficient and adequate controls for their management, and they provide accuracy in and congruence with established policy, process and procedures for grant application processing and administration." Reznick MS utilized a subcontractor, Customer Value Partners, (CVP) to create an Information Technology Audit Report "ITAR".

From our discussions with Reznick MS, and a review of the billings produced by CVP, the OSA was concerned about the stated costs of the CVP "Internal Audit" work as it appeared from the billings from CVP. Subsequent to our field work, OSA was provided information by Reznick MS of their assertions on the component costs of CVP's billings for the stated Internal Audit report. Apparently, the billed costs related to many IT consulting tasks which CVP performed for Reznick MS, but billed under one code. The actual costs of the stated "IT Audit" were not fully determinable.

Regardless, the "ITAR" internal audit report document we reviewed did not appear to meet normal audit standards. The most significant defect of the document was that it was not complete. It appears that the document was designed to contain auditor sign-off blocks in each section indicating that the internal control objectives of that report section were met; however, none of blocks were completed. Also, the document did not include a management letter stating that the objectives of the audit were met, and the name of the internal auditor firm and qualifications of the personnel conducting the review. The language of the SOW created for the IT Audit agreement between Reznick MS and CVP states the case of need for an Internal IT Audit, and that this work would be fulfilling that need.

CVP was noted to have a significant role in the creation of IT systems and methodology with Reznick MS, and therefore, it would appear to be a conflict of interest to also perform internal audit duties for the same processes CVP helped create.

In our post audit discussions with Reznick MS, Reznick has asserted that an IT Audit was not required by the program, and the document and work produced by CVP was not intended to be an internal audit, but was instead additional documentation to assist in the creation of the IT processes at MDA/HAP.

Even though the MDA contract to Reznick MS did not specify an internal IT systems audit, we believe that Reznick MS created an obligation to complete such an audit once it contracted for audit services with CVP and committed MDA funds to this process.

**OFFICE OF THE STATE AUDITOR  
MISSISSIPPI DEVELOPMENT AUTHORITY'S HOMEOWNER ASSISTANCE PROGRAM  
EDP GENERAL CONTROLS AUDIT  
AS OF JULY 31, 2007**

*Recommendation:*

We recommend as an assurance that internal IT controls were functioning as designed, and in consideration that Reznick MS had committed significant funds of the MDA/HAP program to CVP to create an IT Internal Audit Report, that Reznick MS provide the MDA/HAP program a completed and signed Internal Audit report at no additional cost to the program.

**End of Report**