



**STATE OF MISSISSIPPI**  
HALEY BARBOUR, GOVERNOR  
**MISSISSIPPI DEVELOPMENT AUTHORITY**  
LELAND R. SPEED  
EXECUTIVE DIRECTOR

September 30, 2011

Mr. Stacey E. Pickering, State Auditor  
Office of the State Auditor  
Post Office Box 956  
Jackson, MS 39205

**SUBJECT:** Compliance with limited assessment of the Information System (IS) general controls and application controls of the Mississippi Development Authority as focused on the adequacy of MDA's information technology general controls (ITCG).

Dear Mr. Pickering:

The purpose of this correspondence is to transmit the Mississippi Development Authority's response regarding the September 7, 2011, Audit of the MDA IS. The Mississippi Development Authority (MDA) is committed to complete compliance with the findings outlined within this audit. MDA trusts that the following responses are satisfactory to resolve these findings.

**Finding No. 1:** MDA Should Delete Users-ID's of Separated Employees from the Current Active Directory Listings

**MDA Response:** Approximately one year prior to this audit, MDA developed and implemented a procedure and system using an existing task tracking system to notify all key employees and divisions of the announcement of employees planning to leave the employ of the agency. This notification includes Information Technology Division in order to set absolute deadlines for the discontinuance of all network and email access to MDA's Active Directory by the departing employees. It is the practice that all access is ended at the time and date specified by the departure notification. Because it is the practice of MDA IT to keep that "account" active in the directory for 30 days after the employee's departure date, the names associated with those employees still appear in the active directory even though access is routinely ended at the time of departure. The former employee has no access to his account, but the account remains active so the former employee's supervisor may be given access to the account should a need arise after that employee's departure date.

Mr. Stacey E. Pickering, State Auditor

Page 2

September 30, 2011

The current policy, procedure and practice is to remove all access from the Current Active Directory and within 30 days of separation remove the former employee totally from the active directory. MDA believes these actions have adequately addressed Finding No. 1.

**Finding No. 2:** MDA Should Set Expiration Parameters for All Individuals Active Directory Passwords

**MDA Response:** This is a basic security policy which was in effect prior to the audit by the State Auditor's office. One employee, the lead system analyst who is no longer with the agency and who had left his employment prior to this audit, had set a non-expiring password on his own access to the network. This access has been revoked and we are now in compliance with this deficiency. The Network Administrator is now responsible for self-auditing all password expiration dates. MDA does have an application, Priority-One, which has non-expiring accounts but these are restricted accounts, only allowing access to specific data involving Priority-One system. Service Account Functions on MDA servers are non-expiring and will remain that way. These are not user accounts. These accounts are used by the servers to access other servers. Access to these accounts requires passwords with a minimum of 64 characters which are recognized as a part of our security plan.

MDA took corrective action in removing the existing access and enforcing its existing policies and procedures. MDA believes these actions have adequately addressed Finding No. 2.

**Finding No. 3:** MDA Should Develop Formal Documentation For Its Grants Management System 2007

**MDA Response:** Documentation for the Grants Management System did and does exist. It is written into the code for the software application. This is a common practice by programmers to enable a programmer other than the one developing the application to be able to make changes to the package. This documentation is being extracted from the code in the program and it will reside in the IT digital library.

There is also a Users' Manual for the GMS package, a copy of which is housed in the IT digital library (See Attachment 1). MDA believes these actions have adequately addressed Finding No. 3.

**Finding No. 4:** MDA Should Create a Disaster Contingency Plan for IT Services

**MDA Response:** The MDA maintains a Continuity of Operation Plan (COOP). This plan includes documentation for each Division within the agency including IT. (See Attachment 2).

Mr. Stacey E. Pickering, State Auditor

Page 3

September 30, 2011

MDA is also in the process of implementing a multi-phased plan to create total website and data redundancy in an offsite location. The first two phases of a complete back-up of MDA website and MDA servers is in the process of being implemented. The first phase will be the implementation of a fully live, fully redundant Mississippi.org web server in a remote location. This will be completed within 30 days of the date of this letter. Once this is implemented and functioning MDA will begin the process of placing a back-up appliance in a remote location in order to create a live back-up of all data on MDA servers. This appliance will be accessed by the state's backbone. This is a redundant system that will create a mirror of MDA's on-site data back-up in an off-site location. Implementation of this plan is also imminent. MDA IT will also plan to create a completely redundant server cluster structure in this remote location to provide complete redundancy outside of the existing electrical grid and outside of a 100-mile radius of its current location.

MDA believes these actions have adequately addressed Finding No. 4.

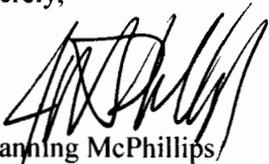
**Finding No. 5:** MDA Should Install Network Banners on Their Internal Network

**MDA Response:** MDA was out of compliance with this finding. MDA took corrective action applying the banner in the start-up script of all MDA computers. IT will push the policy down to the all agency users and computers on October 3, 2011.

MDA believes these actions have adequately addressed Finding No. 5.

The Mississippi Development Authority takes the security and functionality of its technology, hardware and data very seriously. For this reason the agency has made every effort to fully comply with all of the findings of this audit. The responsibility for the operation and maintenance of MDA's computer network system is the number one priority of MDA IT. It is for this reason that MDA will continue to make every effort to adhere to both the spirit and the letter of rules, regulations and laws governing these systems.

Sincerely,



J. Manning McPhillips  
Chief/Administrative Officer

JMM:JH:sw

Attachment