
September 16, 2008

Stacey E. Pickering, State Auditor
Office of the State Auditor
State of Mississippi
P.O. Box 956
Jackson, MS 39205-0956

Dear Mr. Pickering:

The Mississippi Department of Information Technology Services (ITS) appreciates the thorough MVS review conducted by Mr. Toby Frazier and his team. Our goal is to make sure that the State of Mississippi meets the security standards necessary to protect our citizens. Our responses to the assessment findings are listed below.

AUDIT FINDINGS:

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

Response:

We concur with this finding.

Corrective Action Plan:

A. We have addressed the one set of MVS system parameters needed to comply with industry standard security parameters. A system IPL will be required on our five mainframe systems to implement the corrective action.

B. Mitchell Bounds, ITS Data Services Director
Harold Rule, RACF Administrator

C. All five systems have been IPL'd and are compliant as of September 21, 2008.

D. N/A

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

Response:

The Federal auditors work directly with the agency being audited and indirectly with ITS. ITS assists the agency being audited and evaluates, documents, and responds to any findings that are forwarded to ITS. Those responses are sent back to the agency to be included in their responses to the Federal audit findings. We are always available to address any follow-up issues to our responses the agency receives back from the Federal auditors.

Corrective Action Plan:

A. The Office of the State Auditor should require all agencies being audited by the Federal Government to forward all follow-up responses received from the Federal auditors that pertain to ITS back to ITS for further review.

B. Mitchell Bounds, ITS Data Services Director
Harold Rule, RACF Administrator

C. N/A

D. N/A

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

Response:

We acknowledge that this is a concern. However, due to the risk involved in a Disaster Recovery scenario and the limited number of only three systems personnel allowed not to have an expiration date, we feel it is still necessary. The current standard expiration interval for all other mainframe users is thirty days.

Corrective Action Plan:

A. We have changed all users to the thirty day expiration interval except for three systems programmers that would be tasked with recovering the state data center should we experience a disaster.

B. Mitchell Bounds, ITS Data Services Director
Harold Rule, RACF Administrator

C. N/A

D. We do not want to risk the possibility that these three would be unable to recover the systems at a business recovery center because their passwords might be expired. Having an id/password sealed in a envelope to be used in the event of a disaster could become a disaster in itself due to a previous audit finding requiring any id that has not been used in the past sixty days to be automatically revoked.

ITS Should Update and Alter Access to Key MVS Libraries

Response:

We concur with this finding and have addressed the issue.

Corrective Action Plan:

A. After reviewing the access lists of the key MVS libraries listed, we have removed several ids that had update or alter access to these libraries. Two user-ids that were not listed in the systems group are systems programmers and will retain their access.

B. Mitchell Bounds, ITS Data Services Director
Harold Rule, RACF Administrator

C. Completed

D. N/A

ITS Should Designate an Information Security Officer

Response:

ITS understands and agrees with the findings and subsequent recommendations within this section regarding Information Security.

Corrective Action Plan:

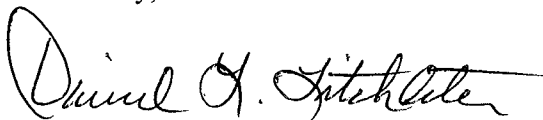
A. ITS will take the necessary personnel actions to establish a focal point within the agency with the primary emphasis and responsibility of maintaining information security for both ITS and the agencies. Once this position is established, a primary function will be to establish a formal security plan that addresses core responsibilities for ITS and provides a template for use by State agencies. ITS will continue to seek funding to assist with the full implementation of the existing security business plan for an Information Security Office with dedicated staffing.

B. David Litchliter, Executive Director
Jimmy Webster, Data Network Manager

C. The implementation of the Office of Information Security will be ongoing.

D. N/A

Sincerely,



David L. Litchliter