mississippi department of
Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

Craig P. Orgeron, Ph.D., Executive Director

Information Systems Management Report

April 15, 2015

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

Dear Mr. Auditor:

The Mississippi Department of Information Technology Services (ITS) is in receipt of the Information Systems Management Report dated March 25, 2015. The report was reviewed by my staff, and we concur with the recommendations set forth in the Control Deficiency findings. Actions have already begun to address the cited deficiencies to improve the State's security posture and to develop documentation specific to the agency's mission. A Corrective Action Plan for each deficiency is listed below.

AUDIT FINDINGS

Agency-Level Efforts for Threat Reduction Should be Expanded

Response:

ITS maintains an Enterprise Security Program with the primary focus of providing resources, guidance, and oversight needed for improving the cybersecurity posture of the Enterprise State Network. ITS maintains enterprise cybersecurity policies, standards, guidelines, and services including the State of Mississippi Enterprise Security Policy (ESP) and Enterprise Security Plan to provide direction and guidance for state agencies as they work to improve their individual agency security posture. ITS directly manages enterprise perimeter security solutions and services that aid in the reduction of cybersecurity risk to Mississippi state agencies utilizing the Enterprise State Network. These solutions and services reduce cybersecurity risk to all state agencies by monitoring and analyzing inbound and outbound network traffic to determine access based on policies, rules, and signatures. ITS regularly reviews the effectiveness of existing security technologies and evaluates new security technologies for protection against emerging security threats.

In addition to maintaining an Enterprise Security Program, ITS has increased its focus on improving the security posture of specific ITS managed systems. ITS, as well as other state agencies, must continue to implement policies, procedures, and solutions to improve the security posture of state government. Although implementing policies and practices that will make the state's systems and data more secure will be an iterative and lengthy process, fully implementing an initial set of actions can help detect and defend against cyber-attacks occurring today and help deter future attacks.

Board Members - Thomas A. Wicker, Chairman • June Songy, Vice-Chairman • D.Shane Loper • Rodney Pearson • J. Keith Van Camp
Legislative Advisors - Senator Sampson Jackson, II • Representative Gary V. Staples

Corrective Action Plan:

A. ITS upgraded the Enterprise State Network perimeter Intrusion Prevention System (IPS) with enhanced features to monitor and analyze inbound and outbound network traffic to determine access based on policies, rules, and signatures. One enhanced feature new to the state is an advanced malware protection feature that assists in identifying and blocking known malware.

B. ITS has implemented the tools and processes required to continuously acquire, assess, and take action on new information in order to identify vulnerabilities and threats and to remediate risks to ITS managed systems; therefore minimizing the window of opportunity for attackers.

C. ITS implemented a new automated monitoring and analysis solution for collecting, correlating, and analyzing computer network security information across the Enterprise State Network. This enhances ITS' ability to notify state agencies participating in the Enterprise State Network of potential cybersecurity activity on State of Mississippi information assets.

D. ITS is developing an internal plan to address the identified gaps in the First Five security controls of the Top 20 Critical Security Controls developed and maintained by the Center for Internet Security (CIS) and the Council on Cybersecurity (CSS). The five security controls are listed below:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges

E. ITS will continue to research and analyze new core and perimeter cybersecurity solutions for improving the cybersecurity posture of the Enterprise State Network.

F. ITS has implemented an ongoing Cybersecurity Awareness Program for ITS staff. ITS also continues to promote a culture of cybersecurity awareness to state agencies and government leaders by encouraging them to consider cybersecurity risks as a priority similar to more traditional risks like financial, safety, and operational. Just as the strongest door and most secure lock will not keep a burglar out if the door is left open or unlocked, the best firewalls and most advanced technology cannot stop a cyber-attack if the individuals using that network are careless, ignorant, or inattentive to basic security practices.

<u>Formal Policies and Procedures Do not Adequately Cover All Areas of Information Technology</u>

Response:

ITS continues to ensure that the ESP is appropriately aligned with current security methodologies. Cybersecurity is a universal concern and failure to adhere to cybersecurity policies can compromise state assets; therefore, compliance to cybersecurity policies must be required. Agencies must have a vested interest in adhering to the cybersecurity policies, guidelines, regulations, and laws (Federal, State, and Local) to demonstrate due diligence to the citizens and businesses that rely on

government services. Compliance with the ESP will provide a baseline of defense, deter a significant number of attacks, and help minimize compromises, recovery time, and costs.

Corrective Action Plan:

1. ITS will expand upon existing documentation and establish specific policies and procedures to address Data Breach Management, Encryption, Access Reviews, and HIPAA regulations for the agency. Once fully vetted, ITS will make these revised policies and procedures available to other state agencies for the development of their own agency specific documents as specified in the Enterprise Security Policy.

2. ITS will continue to promote security awareness training and education for staff, which is recognized as an effective factor in reducing security breaches and data losses.

ITS appreciates the partnership between our agencies and the cooperative work done to improve the State's cybersecurity posture. Given the large and evident risks associated with securing an enterprise network in a decentralized state government environment, it is essential that an enterprise-wide approach to cybersecurity be applied. The success of the enterprise-wide approach is dependent upon the active participation of each state agency associated with the Enterprise State Network. In addition to participating in an enterprise-wide approach to cybersecurity, each agency must also be committed to implementing and maintaining a robust cybersecurity approach to protecting agency owned and operated IT infrastructure. With regard to the IT infrastructure, an interdependent relationship exists for all state agencies, such that strengthening cybersecurity for one strengthens all and, conversely, weakening one weakens all. All state agencies need additional cybersecurity resources (technology, staff, budget authority, etc.) for improving their posture in order to strengthen the posture of the state as a whole.

If you have questions or need additional information, please contact me or Roger Graves of my staff at 601.432.8092 or roger.graves@its.ms.gov.

Sincerely,

Craig P. Orgeron, Ph.D.
Executive Director