JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

PHYLLIS MELLON
ACTING DIRECTOR

October 7, 2010

Doug Ringler, Director
Office of Internal Audit Services
State Budget Office
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48913

Dear Mr. Ringler:

In accordance with the State of Michigan, Financial Management Guide, Part VII, following is a summary table identifying our final response and corrective action plan to address the recommendation contained within the Office of the Auditor General's Performance Audit of Statewide UNIX Security.

Questions regarding the summary table or the corrective action plan should be directed to me at (517) 335-1557.

Sincerely,

Signature Redacted

Michael R. Gilliland, Director
Financial Services

Attachments

c: Mitch Bean, House Fiscal Agency
Trent Carpenter, DTMB
Representative George Cushingberry, Chair, House Appropriations
Laura Hirst, Office of the Auditor General
Senator Mark Jansen
Senator Ron Jelinek, Chair, Senate Appropriations
Nathaniel Lake, Jr., Executive Office
Rick Lowe, OIAS/GSD
Phyllis Mellon, Acting Director, DTMB
David Newman, DTMB Government Affairs
Gary Olson, Senate Fiscal Agency

Statewide UNIX Security
Department of Technology, Management and Budget
Summary of Agency Response to Recommendation
Audit Period: 9/1/08 – 9/30/09

1. Audit recommendation the agency complied with:

   Not Applicable

2. Audit recommendations the agency agrees with and will comply:

   #1 Agrees
   #2 Agrees
   #3 Agrees
   #4 Agrees
   #5 Agrees

3. Audit recommendations the agency disagrees with:

   Not Applicable

Statewide UNIX Security
Department of Technology, Management and Budget
Final Corrective Action Plan
October 7, 2010

**Recommendation #1: Detection of Operation System Weaknesses**
We recommend that DTMB fully develop an effective method to detect operating system weaknesses on UNIX servers.

Agency Response:
DTMB continues to work on process improvements for the UNIX system management by enhancing in house solutions as well exploring open source and commercial solutions to UNIX system management and security.

PCI scans are used by DTMB to assess server security settings from an external perspective. Regular PCI monthly scans are performed on all public facing servers (currently 65 of 549 State of Michigan UNIX servers). Internal servers are scanned on an as needed basis and for the following reasons:

- All new servers are scanned prior to being put into service. The servers must pass a PCI security Scan prior to being put into production.
- Any hosts involved in a firewall rule must pass a PCI security scan.

In addition, number of individual application groups regularly perform PCI scans and review and mitigate findings on a regular basis. As a result of these rules, all internal servers will eventually be PCI compliant too.

DTMB continues to refine its security auditing script. The UNIX team security work group is currently working on adding detection for all DISA level 1 potential vulnerabilities to the UNIX security auditing tool. At this time, with a few noted exceptions (i.e. End of Life Servers and "Appliance" servers), the Unix Security Audit Script has been run on all other servers. Estimated Completion Time for OS Weaknesses Detection on all UNIX servers is September 30, 2011.

Vendor contracts currently require that vendors adhere to all of the State's existing technology standards. A policy has been drafted which requires vendors to resubmit security agreements yearly.

**Recommendation #2 Remediation of UNIX Servers**
We recommend that DTMB fully remediate operating system security weaknesses on its UNIX servers.

Agency Response:
DTMB Technical Services has formed a "Quality Assurance Team" to develop Operating Policies and Procedures for Server Configuration and Security Auditing. This team and members from various other DTMB teams have been

investigating various enterprise software solutions that address System Security auditing, monitoring, and management.

DTMB has been using vendor support contract service days to explore several solutions. DTMB had one of our vendors come in and work with us running a security benchmark tool on a variety of OS platforms. This tool appears to fit our needs for system baseline security reporting on most platforms that Technical Services manages. This tool produces reports in a variety of formats and allows for importing into a larger reporting system. The reports include metrics that will help DTMB track progress in security remediation as well as keeping systems compliant. As an added bonus this tool uses a standard test configuration file that allows it to baseline for a variety of standards.

Central UNIX account management through LDAP would greatly assist DTMB achieve UNIX account security goals. In preparation UNIX staff is currently taking LDAP training though one of our vendors. After which we will start to draw up project plans to implement LDAP UNIX / Linux account management. Estimated completion date for Initial Run of OS Weaknesses Remediation on all UNIX servers is September 30, 2012.

**Recommendation #3: Inventory of Server Information**
We recommend that DTMB improve the accuracy and completeness of information in its UNIX server inventory.

Agency Response:
To help ensure improve and ensure the accuracy of UNIX server inventory, DTMB has requested a Quality Assurance position be created within Data Center Operations (DCO) Configuration Management unit. The position will develop and execute procedures to audit, validate and remediate Configuration Management data for all State of Michigan Information Technology (IT) equipment installed in the hosting centers and remote hosting locations. An Information Technology Programmer / Analyst (ITPA) position was submitted for approval on August 23, 2010. This position should be in place by January 1, 2011.

A "Request to Decommission" procedure has been submitted to the Cross-Functional Review team for approval. We anticipate this will be approved by December 2010. This procedure will help ensure accurate server information is recorded in the CMDB. The Draft procedure for Decommissioning hardware will be used by CMDB staff while we wait for approval on the formal procedure.

Also, changes to the CMDB have been made to accommodate the Application Inventory Repository project, which consists of adding application data into the CMDB. Maintenance of the application data will be handled through the EA Solution Assessment process, DIT-208, and Configuration Item Decommission procedure. This was completed in June of 2010.

**Recommendation #4: Segregation of Duties**
We recommend that DTMB fully establish an appropriate segregation of duties over the administration of all UNIX servers.

Agency Response:
DTMB agrees that segregation of duties is important. To help reduce the risk of a single individual having the authority to bypass critical controls, DTMB continues to pursue transitioning the 7 remaining servers from under Agency Services control to the Technical Services Division. Estimated date of completion for complete segregation of duties over UNIX servers is September 30, 2011.

**Recommendation #5: Server Configuration Procedures**
We recommend that DTMB fully establish procedures for the secure configuration of UNIX servers.

Agency Response:
As part of the overall effort to standardize its system roll out process, DTMB continues to make progress in standardizing server configuration. All new systems are required to go through the standardized system roll out process called Install, Move, Add, and Change or IMAC. The IMAC process will implement many controls including the use of standardized system build images to achieve a more consistent server configuration. Many of the standardized build processes are in place but still need to be formalized in Operating Procedures and Operational Policies. DTMB has on going projects to improve and formalize these processes. Estimated date of completion for standardizing server configuration on all UNIX Servers is March 30, 2012.

DTMB is continuing to develop the existing auditing scripts for regular security testing and exploring other software solutions for UNIX security monitoring to monitor system security settings and to track exceptions and mitigations.

The department continues to develop stronger policies and procedures related to system security, and are working toward enhancing the internal system control policies.