STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

RICK SNYDER
GOVERNOR

DAVID B. BEHEN
DIRECTOR

March 7, 2016

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

Dear Mr. Bankowski:

In accordance with the State of Michigan, Financial Management Guide, Part VII, attached is a summary table identifying our responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of the Department of Technology, Management and Budget, Statewide UNIX Security Controls.

Questions regarding the summary table or corrective action plans should be directed to me.

Sincerely,

Signature Redacted

Michael Gilliland, Director
DTMB Financial Services

c: Senator Dave Hildenbrand, Chair, Senate Appropriations
Representative Al Pscholka, Chair, House Appropriations
Melissa Schuiling, Office of the Auditor General
Jarrod Agen, Executive Office
Dick Posthumus, Executive Office
House Fiscal Agency
Senate Fiscal Agency
Brom Stibitz, DTMB
Rod Davenport, DTMB
Vern Klassen, DTMB
John Juarez, DTMB
Rick Lowe, SBO
David Bates, DTMB
Phillip Jeffery, DTMB
Caleb Buhs, DTMB
Matt Sweeney, DTMB

Department of Technology, Management and Budget
Statewide UNIX Security Controls

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB agrees with and will comply: 1, 2, 3, 4, 5, 6, 7
2. Audit recommendations DTMB fully complied with: None
3. Audit recommendations DTMB disagrees with: None

Agency Responses to Recommendations

1. Improvements to security configuration controls are needed to protect UNIX operating systems.

DTMB agrees with the recommendation and will improve operating system security configuration controls over the State's UNIX server environment. DTMB has purchased the necessary automation tools and has initiated a project to enforce and maintain effective standardized Operating System security configuration controls. The department will fully comply by June 2017.

2. Establishment of approved UNIX operating system versions are needed to protect confidential and critical information residing on State systems.

DTMB agrees with the recommendation and will establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications. DTMB will utilize the Enterprise Architecture Roadmap to identify authorized and supported operating systems. DTMB has already begun issuing owners of unauthorized and unsupported operating systems a "Notice of Non-Compliance" and is working with the responsible departments to replace these systems. DTMB will ensure new operating system installations comply with the Enterprise Architecture Roadmap. In addition, DTMB is implementing a new IT infrastructure, the Next Generation Digital Infrastructure (NGDI), which will define acceptable UNIX operating systems and require State executive branch departments transitioning to the NGDI to use these operating systems. The department will fully comply by December 2016.

3. Improved patch management controls would help protect State applications from known vulnerabilities and ensure data integrity.

DTMB agrees with the recommendation and will use an automated patch management control process and tools to patch servers, at a minimum quarterly, and run reports to identify any deficient patches. In addition, the department will establish and implement a memo of understanding (MOU), with all executive branch agencies, to define mutually agreed upon patch management maintenance windows. Lastly, the department will enforce DTMB procedure 1345.00.50.08 on Server Patch Management, to ensure servers are patched timely, with any exceptions receiving a "Notice of Non-Compliance" which will be reported for further resolution. The department will fully comply by December 2016.

4. Improvements needed to UNIX operating system access controls.

DTMB agrees with the recommendation and has updated its elevated user rights procedure to more effectively control access to the UNIX operating systems. In addition, the department is in the process of implementing an elevated rights and directory services software tool; updating associated access procedures; developing new reports and monitoring processes to further strengthen UNIX operating system access controls and ensure compliance with DTMB policy. The department will fully comply by December 2016.

5. Enhancements to procedures for detecting and remediating security vulnerabilities are necessary.

DTMB agrees with the recommendation and the department has purchased the necessary automation tools and initiated a project to install the tools on all UNIX servers. The new tools will automate the detection and remediation of security vulnerabilities. The department is developing a process to assign responsibilities, between Technical Services, Agency Services and Network and Telecommunication Division, for the remediation of threats detected in vulnerability scans. In addition, the department will utilize existing server management standards, new vulnerability scan procedures, new monitoring processes, and new operational compliance reports to enhance the detection and remediation of security vulnerabilities. All procedures will be reviewed at least annually, to meet industry best practices. The department will fully comply by June 2017.

6. Segregation of duties could help ensure that critical operating system controls cannot be bypassed.

DTMB agrees with the recommendation and has begun an analysis of segregation of duties over the administration of UNIX servers. The department will fully comply by June 2016.

7. Inventory management improvements are needed to ensure that critical decisions can be made in a timely manner for the State's information systems.

DTMB agrees with the recommendation and has procured an automated inventory management tool which is in the process of being fully implemented. The automated inventory management tool will automatically confirm and update the State's information systems inventory data in the CMDB. Data collection will begin by June 2016 and the department will fully comply by June 2017.