STATE OF MICHIGAN

RICK SNYDER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

DAVID L. DEVRIES
DIRECTOR

December 17, 2018

Mr. Rick Lowe
Office of Internal Audit Services
Office of the State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48913

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, following is a summary table identifying our ongoing 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 Windows Active Directory Environments.

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

Sincerely,

Signature Redacted

Mr. David L. DeVries
Director and State CIO
Department of Technology, Management and Budget

cc: Executive Office
Representative Laura Cox, Chair, House Fiscal Agency
Senator Dave Hildenbrand, Chair, Senate Fiscal Agency
Melissa Schuiling, Office of the Auditor General
House Fiscal Agency
Senate Fiscal Agency

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB fully remediated: 1, 7, 9, 11, 12, 13, 14, 15, 16
2. Audit recommendations DTMB agrees with and will continue to remediate: 2, 3, 4, 5, 6, 8, 10
3. Audit recommendations DTMB disagrees with: None.

Agency Responses to Recommendations

Finding #1 - Sufficient governance needed to protect Active Directory

DTMB agreed with the recommendation and instituted effective governance over the Active Directory (AD) environment. DTMB completed remediation in November 2018.

- DTMB developed an AD Governance Board in October 2017 with a signed charter (June 2018). The AD Governance Board's first meeting was in October 2017. The AD Governance Board currently meets monthly to address the audit issues.
    - The AD Governance Board assessed and identified Standards relevant to the secure administration of Active Directory. DTMB formalized an enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).
    - The Active Directory Governance Board will evaluate whether separate forests and associated trusts are still required as part of the annual memorandum recertification.
- DTMB is implementing a Security Accreditation Process (SAP) and uses an automated Governance Risk and Compliance platform to enable the process. Adopted from processes currently in place at Federal agencies in accordance with NIST and other best practices, it provides a risk management process to manage the attendant IT security risks to businesses. DTMB completed a system security plan (SSP) for Active Directory as part of the overall risk assessment of the SOM NGDI environment which includes the Active Directory component. DTMB included MiID as a component in the SOM NGDI ATO and associated risk assessment. The State's CIO issued the Final Authority to Operate for SOM NGDI on August 31, 2018.
- DTMB assessed the Microsoft Risk Assessment and remediated security issues that were of value to the State of Michigan's Active Directory environment. DTMB is focusing on improving the security and operations of Active Directory as part of the implementation of the SSP's Plan of Action and Milestones in accordance with the State's Security Accreditation Process.
- DTMB follows the State's formal change management process. An updated EASA was approved to cover all State AD environments (June 2017).

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #2 - Establish and implement baseline configurations

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in January 2019.

- Active Directory Governance Board adopted the framework DTMB uses as a basis for configuring and securing the State's Active Directory domain controllers in the new enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).

  - o The Active Directory Governance Board developed and approved the Active Directory domain controller baseline configurations (May 2018).
    - The Active Directory domain controller baseline configurations will be reviewed and recertified on an annual basis by the Active Directory Governance Board, as outlined in the new enterprise Active Directory Account Management Standard 1345.00.30.
- The Active Directory Governance Board will develop and document a process to monitor the Active Directory administrative owner's compliance with the approved baseline configurations (January 2019).

Finding #3 - Improvements needed in monitoring security events and securing event logs

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in March 2019.

- Active Directory Governance Board assessed and identified high-risk AD security events to monitor. DTMB included these events in the new enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).
- All Active Directory administrative owners, including the separate State Agency, established alerting on the high-risk security events identified in their Active Directory Account Management Standards (August 2018).
- All Active Directory administrative owners, including the separate State Agency, will establish and implement an approved internal procedure to follow-up on the alerts and implement independent monitoring of privileged administrator activity; estimated completion March 2019.

Finding #4 - Active Directory consolidation may improve security

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation will be completed in December 2018. DTMB is performing the following actions:

- The Active Directory Governance Board assessed the existing domains and identified 4 additional domains that will be consolidated (November 2018).
- Active Directory Governance Board will develop, approve, and formalize an MOU with Active Directory administrative owners if it is determined the Active Directory environment should not be consolidated into DTMB's Active Directory environment; anticipated completion December 2018. The migration plans for consolidation will be scheduled as part of a formal project.

Finding #5 - Improvements to the Configuration Management Database needed to ensure availability of information

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in March 2019.

- DTMB and the separate State Agency performed a clean-up of specific issues cited in the audit report. (August 2018)

- Active Directory administrative owners are defining and implementing an internal process to ensure the State's Configuration Management Database (CMDB) is regularly updated for required AD fields; anticipated completion March 2019. The separate State agency maintains its own CMDB.

Finding #6 - Monitoring needed to ensure the separate State agency and a vendor follow State standards

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in December 2018.

- DTMB and the separate State Agency are developing a partnership agreement (PA). The PA will identify the uniqueness of each partner and their roles and responsibilities, and the requirement of each partner to maintain and comply with their NIST based PSPs; anticipated completion end of December 2018. The separate State Agency is part of the Active Directory Governance Board.
- DTMB implemented a process to verify the vendor supporting one AD environment implements Active Directory controls in compliance with relevant State standards (July 2018). The vendor's contract contains language that specifies the vendor must adhere to State standards.

Finding #7 - Training program improvements needed

DTMB agreed with the recommendation and completed remediation in February 2018.

- DTMB Active Directory system administrative owners developed an internal standard based on NIST SP 800-16, which defines the training requirements and evaluation criteria. (February 2018)
- DTMB Active Directory system administrative owners implemented processes to maintain formal training records. (February 2018)

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #8 - Improvements in domain configurations needed to protect Active Directory

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in December 2018. DTMB is performing the following actions to remediate the finding:

- Active Directory system administrative owners, including the separate State Agency, are implementing the approved AD Baseline Configurations on their AD domain controllers; anticipated completion December 2018.
- The Active Directory Governance Board developed a list of the approved Active Directory authorized services (September 2018).

Finding #9 - Improved controls over administrative access would help reduce the risk of unauthorized access

DTMB agreed with the recommendation and completed remediation in December 2018.

- The AD Governance Board assessed and identified Standards relevant to the secure administration of Active Directory. DTMB formalized an enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).
- The separate State Agency developed a procedure governing the use of the Active Directory default administrative account (August 2018).
- Active Directory system administrative owners, including the separate State Agency, assessed and updated administrative password controls (September 2018).
- Active Directory system administrative owners, including the separate State Agency, implemented fine-grained password policies or using multi-factor authentication for privileged user accounts (November 2018).
- Active Directory system administrative owners perform periodic recertifications of administrative user access rights to ensure the access rights administrators have are appropriate (August 2018).

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #10 - Improved non-user account management needed to reduce the risk of unauthorized access

DTMB agreed with the recommendation and will continue to remediate. DTMB anticipates the remediation to be completed in March 2019. DTMB is performing the following actions to remediate the finding:

- The AD Governance Board assessed and identified Standards relevant to the secure administration of Active Directory. DTMB formalized an enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).
    - DTMB recertify non-user accounts in accordance with this Standard. Active Directory system administrative owners are only responsible for recertifying accounts in predefined or delegated group within Active Directory. Other non-user accounts are authorized and recertified by the application/service requesting the account as addressed through application specific SSP's.
    - The separate State Agency recertifies their AD non-user accounts in accordance with the separate State Agency's Standard. (April 2018)
- DTMB deployed a solution to manage non-user accounts, including a process for changing non-user account passwords (December 2018). DTMB also creates managed service accounts to randomly change passwords when appropriate.
- DTMB and the separate State Agency are restricting non-user accounts to specific resources (December 2018).
- DTMB updated internal procedures to require all Active Directory non-user accounts to have a password (April 2017).
- DTMB is updating internal procedures to ensure proper management of non-user account passwords (March 2019). DTMB will incorporate this practice into the State enterprise technical standards (April 2019).

Finding #11 - Improved user account password parameters would help reduce the risk of data breaches

DTMB agreed with the recommendation and completed remediation in October 2018.

- DTMB and the separate State Agency analyzed and remediated user accounts to ensure the accounts are configured in accordance with the State's password requirements (October 2018).

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #12 - Antivirus protection needed to safeguard against malicious code

DTMB agreed with the recommendation and completed remediation in October 2018.

- The Active Directory administrative owners cited in the audit report deployed antivirus in their Active Directory environments (October 2018).

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #13 - Timely patches needed to ensure domain controller security

DTMB agreed with the recommendation and completed remediation. DTMB implemented processes to patch the cited Domain controllers (February 2018). DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #14 - More effective user account management needed

DTMB agreed with the recommendation and completed remediation in November 2018.

- The AD Governance Board assessed and identified Standards relevant to the secure administration of Active Directory, including recertification of AD user accounts and disabling inactive AD accounts. DTMB developed an enterprise Active Directory Account Management Standard (1345.00.30); (August 2018).
- DTMB performs user recertifications in accordance with the procedure described in the new enterprise Active Directory Account Management Standard (1345.00.30) (November 2018). In addition, DTMB performs a weekly match of employee accounts to HRMN.
- The separate State Agency recertifies their AD user accounts in accordance with the separate State Agency's Standard. (April 2018)
- DTMB disables inactive user accounts in accordance with the procedure described in the new enterprise Active Directory Account Management Standard (1345.00.30) (September 2018).
- The separate State Agency investigates inactive user accounts in accordance with the separate State Agency's Standard. (July 2018)
- DTMB maintains a listing of the Active Directory authorized requestors. DTMB documents the authorization to create Active Directory accounts using MiID or the DTMB-161 form.

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #15 - Periodic account recertification needed

DTMB agreed with the recommendation and completed remediation in November 2018.

- The AD Governance Board assessed and identified Standards relevant to the secure administration of Active Directory, including recertification of AD user accounts and disabling inactive AD accounts. DTMB formalized an enterprise Active Directory Account Management Standard (1345.00.30) (August 2018).
- DTMB performs user recertifications in accordance with the procedure described in the new enterprise Active Directory Account Management Standard (1345.00.30) (November 2018). In addition, DTMB continues to perform a weekly match of employee accounts to HRMN.
- The separate State Agency recertifies their AD user accounts in accordance with the separate State Agency's Standard. (April 2018)

DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #16 - Improvements needed to record retention and disposal schedule

DTMB agreed with the recommendation and completed remediation in August 2018.

- DTMB retains Active Directory user request records in accordance with the State's Records Management General Schedule 5.34. DTMB formalized an internal Procedure governing the retention of related records (July 2018).

DTMB recommends this finding be closed based on the effective design of DTMB's controls.