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, Network and Cyber Security.

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 Response to Recommendations

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

Agency Responses to Recommendations

Finding #1 - Need to fully establish and implement configuration management controls

DTMB partially agreed with the recommendation and remediated the parts DTMB agreed with in September 2018.

- DTMB formalized a published internal standard adopting the framework DTMB uses as a basis for configuring and securing the State's network devices. The standard was signed on May 15, 2018.
  - Held kick-off meetings with Network managers and SMEs (June 2018)
- DTMB formalized its processes for configuring and securing the network devices into a published internal procedure. The procedure was signed on May 15, 2018.
  - Established a review and approval process (May 2018)
  - Established a repository to store approved configuration templates (June 2018)
  - Populated a repository with initial approved configuration templates (June 2018)
- DTMB formalized a published internal procedure to review and monitor the network device configurations (July 2018).
- DTMB expanded its monitoring of security configuration settings on network devices (September 2018).

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

Finding #2 - Network Access Control (NAC) solution needed to help prevent unauthorized devices from connecting to the State's network

DTMB partially agreed with the recommendation. DTMB began a deliberate enterprise implementation of NAC in May 2018. Consisting of hardware modernization as well as NAC configuration, completion of the NAC enterprise implementation is anticipated by the end of December 2019.

DTMB's implementation of the NAC project will also prevent the risk of rogue access points connecting to the State's wired network.

Finding #3 - Improved process needed for managing updates to network device operating systems

DTMB agreed with the recommendation and completed remediation in June 2018. DTMB formalized a published internal procedure for analyzing network security vulnerabilities which was signed May 2018. DTMB is using the newly documented procedure to manage updates to the operating systems of network devices.

  - Established workflow for review and approval (June 2018)
  - Established location to store the results of the review (June 2018)

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

Finding #4 - Network device lifecycle management processes need improvement
DTMB agreed with the recommendation and completed remediation in December 2018. DTMB formalized a published internal procedure for the lifecycle management of network devices which was signed in May 2018.

DTMB uses a risk-based approach to replace devices on a continual basis. Beginning in 2015, DTMB implemented enterprise projects to heighten the priority of the replacement schedule to methodically replace all key infrastructure components. Using a risk-based approach, DTMB started by replacing core and border network devices. In 2016 and 2017, DTMB further evaluated network infrastructure equipment and replaced additional core network infrastructure devices.

DTMB has a five-year lifecycle for network devices; approximately 20% of its network devices would be replaced each year. Since October 2017, DTMB replaced approximately 470 network devices as part of DTMB's ongoing State LAN network device technology refresh as well as break/fix replacements and will continue to replace as funding is available.

DTMB expanded the enterprise CMDB capability to include the network devices which are consumed from the separate tool suite which currently tracks network devices (December 2018). DTMB developed capability to produce network device lifecycle management reports (October 2018).
DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #5 - Security training program improvements needed
DTMB agreed with the recommendation and completed remediation in August 2018.

- DTMB established a location to store historical training records for individuals with network security roles and responsibilities (June 2018) and is storing the records in the established site.
- DTMB established a training matrix by skill set and level to track available and required training (August 2018).

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

Finding #6 - Procedures need to be more fully developed and implemented
DTMB agreed with the recommendation and completed remediation in May 2018.

DTMB assessed, identified, and documented additional network procedures and implementation guidance to address a variety of controls for securely managing the network. Specifically, DTMB developed and signed the following additional internal procedures and Standard:

- Procedure - Network Configuration Management; signed May 14, 2018
- Procedure - DTMB ACS System Administrator Account Access Review; signed May 15, 2018
- Procedure - DTMB RSA SecurID System Administrator Account Access Review; signed May 15, 2018
- Procedure – Network Vulnerability Remediation; signed May 15, 2018
- Procedure - Network Infrastructure Lifecycle Management; signed May 16, 2018
- Standard – Network Security Control List; signed May 16, 2018

DTMB recommends this finding be closed based on the remediations DTMB performed.

Finding #7 - Complete information needed to track and manage network devices

DTMB partially agreed with the recommendation and remediated the parts DTMB agreed with in February 2018.

- DTMB refined the purpose and scope of the operational inventory system cited in this finding through an internal standard. The standard identifies which fields are required and provides the linkage to other authoritative systems that contain sensitive data elements.
- DTMB reviewed the data elements in the inventory system and remediated the items (February 2018)

DTMB recommends this finding be closed based on the immediate remediations DTMB performed.

Finding #8 - Controls over firewalls need to be improved to ensure security of the network

DTMB agreed with the recommendation and completed remediation. DTMB implemented the following enhancements to the process to provide effective management over firewall rules.

- DTMB automated the request, change management, and approval process of firewall rules which will provide the documentation. In addition, DTMB continually improves the documentation, review, and approval of firewall rulesets. This additional capability has been in operation since January 2018.

DTMB's leadership review concluded reviewing older existing firewall rulesets would not be of significant benefit, given the costs of performing the review; a review of older existing firewall rulesets is very manpower intensive. As mitigation strategy, DTMB is aggressively moving effected servers into the State's Next Generation Digital Infrastructure (NGDI). As systems move into NGDI, older firewall rules will be decommissioned. Expected completion of the older systems into NGDI is by end of Fiscal Year 2019.
DTMB recommends this finding be closed based on the effective design of DTMB's controls.

Finding #9 - Improvements in network device configurations needed

DTMB agreed with the recommendation and remediated most of the network device operating system baseline configuration exceptions DTMB agreed with.

- Written internal policy, signed May 15, 2018, prescribes the related configuration management standard and procedures to ensure the configuration of network device operating systems are in concert with vendor hardening recommendations.
- DTMB Subject Matter Experts (SMEs) evaluated the effect and impact the remaining baseline configuration exceptions have on the State's network.
    - DTMB developed plans to remediate the remaining configurations.
    - DTMB remediated the less complex network configurations. The more complex remaining configurations (less than 4% of sampled configurations) will be prioritized with other network device lifecycle modernization projects;
      these are planned to be completed by the end of March 2019 due to restrictions on

network changes during the November election period and necessary external coordination.

Finding #10 - Improved controls over administrative access would help reduce the risk of unauthorized access

DTMB agreed with the recommendation and completed remediation by documenting an effective control process for administrative access to State network devices. DTMB also executed corrections to many privileged network administrator's access during the audit and remediated the remaining issues.

- DTMB established the location to store the administrative user access reviews (June 2018).

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

Finding #11 - Risk management practices not fully established and implemented

DTMB agreed with the recommendation to establish and implement effective risk management practices over the State's network to help ensure security risks are identified and sufficiently evaluated. DTMB will continue remediation and anticipates the remediation will be completed in December 2019.

DTMB is implementing a Security Accreditation Process 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. Phase 1 of the implementation concluded at the end of fiscal year 2018. Phase 2 implementation coincides with the State's 2018 Internal Control Evaluation cycle.

DTMB's Vulnerability Management Program uses a variety of tools to identify vulnerabilities from its network devices. DTMB is improving its network vulnerability scanning process with new capabilities recently obtained. DTMB continually takes a risk-based approach to improve the scanning processes using new capabilities and procedures. DTMB evaluated using a combination of authenticated and unauthenticated scanning (September 2018). DTMB is executing a project plan expanding network device vulnerability scanning; estimated completion by the end of December 2019.

DTMB Cyber Security already has penetration testing services available for use as needed. Each year since its implementation in 2016, DTMB and Agencies have been using the contract to test and remediate information systems. Additionally, DTMB updated SUITE with cyber security check points including specific security testing which includes scanning of application code, identifying the application vulnerabilities and mitigating prioritized vulnerabilities. The summary results will be stored within the Governance, Risk and Control platform using the Michigan Security Accreditation Process (MiSAP).

Finding #12 - Improvements needed over network monitoring

DTMB agreed with the recommendation and completed remediation in September 2018. DTMB performs network event monitoring, correlating information from 1800 different sources to identify and analyze security events. This allows for an effective approach to analyze security events.

- DTMB established a process to assess and remediate high-risk network security events when required (May 2018).
- DTMB documented the high-risk network security events DTMB actively monitors (September 2018). DTMB continues to refine the monitored high-risk network security events.

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

Finding #13 - Monitoring process for unauthorized wireless access points needs to be fully implemented

DTMB agreed with the recommendation because DTMB has always maintained effective access controls over the State's wireless network that protect against threats presented by unauthorized wireless access points. DTMB is proactively restricting the devices which can access the State's wired network with the Network Access Control solution DTMB is implementing to address finding #2.

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

Finding #14 - Security awareness training program should continue

DTMB agreed with the recommendation and will continue its strong cyber security awareness program.

DTMB is working with the necessary State agencies to make this annual certification training required of all State employees. Initial employment and annual cybersecurity awareness training will be required to have access to the State's network. DTMB anticipates initial operating capability to track individual's annual training by the end of March 2019.