Office of the Auditor General
Performance Audit Report

Network and Cyber Security
Department of Technology, Management, and Budget

March 2018

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

071-0518-17

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Network and Cyber Security

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0518-17

Released:
March 2018

Network security refers to any activity designed to protect the availability, confidentiality, and integrity of a network and data. It includes implementation of hardware and software technologies to help secure the network. Cyber security is the practice of defending an organization's network, computers, and data from unauthorized access, attack, or damage by implementing secure processes and technologies. Within DTMB, network and cyber security are primarily the responsibility of the Network and Telecommunication Services Division, Michigan Cyber Security, Design & Delivery, and Technical Services.

Audit Objective	Conclusion
Objective #1: To assess the sufficiency of DTMB's efforts to design and administer a secure IT network.	Moderately sufficient

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB needs improved configuration management controls. These controls directly impact DTMB's ability to protect the State's network from threats and vulnerabilities (Finding #1).	X		Partially agrees
DTMB did not implement a network access control solution to help ensure that only authorized devices access the State's IT network and that unauthorized or unmanaged devices are detected and prevented from connecting (Finding #2).	X		Partially agrees
DTMB did not fully establish and implement an effective process for managing updates to the operating systems of network devices. We identified 10 vulnerabilities classified as high or medium severity that should be remediated (Finding #3).	X		Agrees
For 19% of the State's network devices, DTMB did not ensure that the devices were supported by the vendor. Also, 45% of network devices were not approved for use in the State's IT environment (Finding #4).		X	Agrees
DTMB needs to improve its training program to ensure that individuals responsible for securing the network receive adequate security-related training necessary to perform their assigned duties (Finding #5).		X	Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not fully develop and implement comprehensive formal procedures to address a variety of controls for securely managing the network. Complete procedures were not developed and implemented for items such as firewall management, configuration management, user access, and security event monitoring (Finding #6).		X	Agrees
DTMB's operational inventory of network devices did not contain complete information, which could negatively impact security management. The device inventory did not always identify device type and operating system version (Finding #7).		X	Partially agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DTMB's security and access controls over the State's IT network.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Firewall rulesets were not periodically reviewed, tested, and monitored to help protect the State's network from threats and ensure that firewalls are operating as intended to prevent unauthorized access (Finding #8).	X		Agrees
DTMB did not configure network device operating systems in accordance with best practices. We noted configuration exceptions on 100% of the devices reviewed (Finding #9).		X	Agrees
DTMB did not fully establish a variety of access controls over the State's network devices, increasing the risk of unauthorized changes that could disrupt the stability and compromise the security of the network (Finding #10).		X	Agrees

Audit Objective	Conclusion
Objective #3: To assess the sufficiency of DTMB's efforts to monitor the security of the State's IT network.	Moderately sufficient

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not conduct a risk assessment and fully implement an effective process for identifying and remediating vulnerabilities on network devices. Authenticated and unauthenticated vulnerability scans were not conducted on 45 and 39, respectively, of the 45 sampled devices (Finding #11).	X		Agrees
DTMB did not monitor all high risk network security events and did not always properly secure access to network monitoring tools (Finding #12).		X	Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not detect and investigate unauthorized wireless access points to ensure that the State's IT network is protected against threats (Finding #13).		X	Agrees

Audit Objective	Conclusion
Objective #4: To assess the effectiveness of DTMB's cyber security awareness programs.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB should continue its cyber security awareness training program. DTMB should also take steps to ensure that all information system users participate in the cyber security awareness training program. An average of 68% of State employees participated in each of the 24 training lessons (Finding #14).		X	Agrees

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

This Page Left Intentionally Blank

OAG
Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

March 16, 2018

Mr. David L. DeVries
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. DeVries:

This is our performance audit report on Network and Cyber Security, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

NETWORK AND CYBER SECURITY

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

DESIGN AND ADMINISTRATION OF A SECURE IT NETWORK

BACKGROUND

Network security refers to any activity designed to protect the availability, confidentiality, and integrity of an IT network and data. The State of Michigan (SOM) network encompasses all aspects of wired and wireless components, including computers, servers, network devices, and other technologies and the data that the State stores and transmits.

The Department of Technology, Management, and Budget's (DTMB's) Michigan Cyber Security (MCS) unit is responsible for defining security* roles and responsibilities within DTMB's IT governance framework, establishing a disciplined strategy and response to security incidents, and providing a universal computer security risk management practice. The Network and Telecommunication Services Division's (NTSD's) mission is to provide highly efficient and cost-effective managed network services to all SOM agencies and their clients. Some of NTSD's primary responsibilities include the design, configuration*, and maintenance of network devices such as routers, switches, and firewalls*.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to design and administer a secure IT network.

CONCLUSION

Moderately sufficient.

FACTORS IMPACTING CONCLUSION

- Network availability reports indicated a generally stable and available network.
- Network topology diagrams were generally complete and accurate.
- Three material conditions* related to fully establishing and implementing configuration management* controls, implementing a network access control solution, and managing updates to operating systems of network devices (Findings #1 through #3).
- Four reportable conditions* related to establishing and implementing effective lifecycle management processes, improving the security training program, developing and implementing comprehensive formal procedures for securely managing the network, and ensuring completeness of the network device inventory (Findings #4 through #7).
- Deficiencies in network design and administration contributed to the material and reportable conditions under Objectives #2 and #3.

** See glossary at end of report for definition.*

FINDING #1

Need to fully establish and implement configuration management controls.

DTMB had not fully established and implemented configuration management controls to ensure that the State's network devices are securely configured. Configuration management controls directly impact DTMB's ability to protect the State's network from threats* and vulnerabilities*.

According to the National Institute of Standards and Technology* (NIST), organizations can control vulnerabilities and reduce threats by implementing a robust security configuration management process. Baseline configurations* are important because they ensure that all network devices are properly configured in accordance with the State's reviewed and agreed-upon security requirements.

Specifically, DTMB did not:

a. Create a standard to formally adopt the industry best practices used as a basis for securing network devices.

   For example, the standard would require that network devices be configured according to a specifically identified vendor hardening guide.

   NIST Special Publication 800-128 states that organizations are responsible for adopting secure configurations for an information system and that these configurations should be approved in compliance with organizational policy.

   DTMB informed us that it used vendor-recommended settings and internal subject matter experts as a basis for creating internal configuration checklists* for securing network devices. However, formally creating a standard to adopt industry best practices would help DTMB ensure consistent and appropriate implementation of secure configurations on network devices.

b. Develop internal security configuration checklists for all network devices and ensure that existing internal security configuration checklists were established in accordance with industry best practices.

   SOM Technical Standard 1340.00.060.01 requires that security configuration checklists be used to implement baseline configurations. Any deviations from established secure configurations should be identified, documented, and approved.

   Because of the confidentiality of these configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

** See glossary at end of report for definition.*

c. Implement all baseline configurations in accordance with industry best practices and internal security configuration checklists.

   SOM Technical Standard 1340.00.060.01 requires DTMB to implement baseline configurations that reflect the most restrictive mode consistent with operational requirements. NIST states that, when deviations from industry best practices or security configuration checklists arise, the deviation should be individually assessed and either resolved or documented and approved through the configuration change control process.

   Because of the confidentiality of these configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

d. Establish a formal process to review and update internal security configuration checklists and baseline configurations of network devices.

   According to SOM Technical Standard 1340.00.060.01, baseline configurations should be reviewed and updated:

   - According to the system's configuration management program or at least every 90 days.
   - When required because of a major system change or upgrade.
   - As an integral part of IT component installations and upgrades.

   DTMB informed us that baseline configuration updates were performed as a result of major events* affecting the network infrastructure and that internal security configuration checklists were updated on an as-needed basis; however, formal reviews are not performed every 90 days as required by standards.

e. Establish a process to routinely monitor network device security configuration settings.

   SOM Technical Standard 1340.00.060.01 requires that DTMB monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

** See glossary at end of report for definition.*

According to NIST, organizations should perform security-focused configuration management monitoring, including:

- Scanning to identify deviations between the approved baseline configuration and the actual configuration for an information system.
- Querying audit records or logs to monitor and identify unauthorized change events.
- Running system integrity checks to verify that baseline configurations have not been changed.
- Reviewing change control records (including system impact analyses) to verify conformance with configuration management policy and procedures.

Changes detected as a result of these monitoring activities should be reconciled with approved changes and the results of the monitoring activities should be analyzed to determine the reasons that an unauthorized change occurred.

Network security configurations not sufficiently monitored.

DTMB informed us that it considers the actual configuration of each network device to be the baseline configuration. DTMB also informed us that it monitors changes to the actual configuration of approximately 100 (3%) of 3,876 network devices. However, DTMB should monitor configuration settings for all network devices to ensure that the devices remain in compliance with approved secure baseline configurations.

f. Follow a formal process for testing individual configuration item changes or fully document the detailed results of this testing.

SOM Technical Standard 1340.00.060.01 requires that DTMB test, validate, and document changes to network devices before implementing the changes on the operational system.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of these controls in ensuring the secure configuration of network devices. We determined that the weaknesses in this finding were the cause of Finding #9.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective configuration management controls for the State's network devices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees with the recommendation. DTMB employs a defense-in-depth approach, including effective configuration management controls, that enables DTMB to protect the State's network from threats and vulnerabilities. DTMB's configuration management controls include: continually improved internal security configuration checklists, version-controlled baseline configurations, and operational processes based on the enterprise configuration management standards.

DTMB:

- *Creates security configuration checklists that outline settings for basic configuration and security items. Checklists may be used for multiple device models; they are not always device specific.*

- *Develops baseline configurations for all devices utilizing relevant security configuration checklists and vendor hardening guidelines. The baseline configurations reflect the most restrictive mode consistent with operational requirements. The baseline configurations are maintained in the configuration management system where the baseline configuration can be rolled back if necessary.*

DTMB is formalizing a written internal standard that adopts industry best practices for secure configurations and estimates that it will be completed in April 2018. DTMB has already remediated 96% of the exceptions to date. Using a risk-based approach, DTMB will continue to evaluate improvements to monitoring network device configuration settings.

DTMB disagrees this is a material finding. The implemented configuration management controls help ensure the SOM network is effectively protected from threats and vulnerabilities.

FINDING #2

NAC solution needed to help prevent unauthorized devices from connecting to the State's network.

DTMB did not implement a network access control (NAC) solution to help ensure that only authorized devices access the State's IT network and that unauthorized or unmanaged devices are detected and prevented from connecting. Unauthorized devices may not meet the State's security requirements, increasing the risk of compromise or infection of the network.

NIST states that automated mechanisms should be employed to detect the presence of unauthorized hardware within a network and disable network access for such components. SOM Technical Standard 1340.00.080.01 requires that devices be uniquely identified and authenticated before connecting to the network.

DTMB periodically performs network discovery scans to identify the IP addresses connected as of a point in time. A device may have one or more IP addresses. As of June 2017, approximately 87,000 IP addresses were connected to the State's network. However, DTMB did not implement sufficient processes to determine if each of the connected IP addresses represented authorized devices in the State's various IT hardware inventory systems.

We consider this finding to be a material condition because of the significance of this control and the large number of access points to the State's network.

RECOMMENDATION

We recommend that DTMB implement a NAC solution to help ensure that only authorized devices access the State's IT network and that unauthorized or unmanaged devices are detected and prevented from connecting.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees with this recommendation. DTMB does not have a single automated NAC solution to ensure that only authorized devices access the State's IT network. DTMB is currently conducting a limited pilot to determine the feasibility of implementing a NAC solution.

However, there are numerous approaches to ensure unauthorized or unmanaged devices are detected and prevented from connecting to the State's network. DTMB minimizes the risk of unauthorized devices connecting to the State's network by employing defense-in-depth security controls such as:

- *Beginning February 2016, DTMB disables network ports that are not regularly used.*
- *User authentication is required to access SOM systems and data.*

- *Multifactor authentication is required for Administrative access.*

- *Firewalls protect secure zones by only allowing access to and from specific authorized resources.*

- *DTMB monitors traffic for hacking and infections using Intrusion Prevention System/Intrusion Detection Systems and initiates immediate blocking if attacks are identified.*

DTMB disagrees this is a material condition due to the defense-in-depth processes DTMB practices.

FINDING #3

Improved process needed for managing updates to network device operating systems.

DTMB did not fully establish and implement an effective process for managing updates to the operating systems of network devices. Keeping devices updated will help DTMB protect the network from unintended weaknesses that could allow an attacker to compromise the availability, confidentiality, and integrity of the network.

Hardware vendors release security advisories about network vulnerabilities, including the severity of the vulnerability, details needed to assess the impact, and steps needed to protect a network.

DTMB needs to establish a formal process for assessing the risk that security advisories have on the State's network device operating systems. A formal process would include identifying the impacted network devices, assessing the vulnerability's impact, identifying compensating controls, and determining whether to apply an update.

NIST states that organizations should identify, report, and correct network device flaws using patches, upgrades, or other response activities based on security assessments. SOM Technical Standard 1340.00.03 outlines the remediation time lines for updating devices.

10 vulnerabilities on 1,361 network devices had not been remediated.

We reviewed security advisories for 4 operating system versions running on 1,361 (44%) of the State's 3,126 network devices. We identified 10 (36%) of 28 judgmentally selected vulnerabilities that the vendor classified as high or medium severity that could potentially be exploited in the State's IT environment because DTMB had not remediated them.

DTMB informally reviews security advisories as they are released and determines the action necessary based on the risk posed to the State. However, DTMB was unable to provide evidence supporting that it had performed a security impact analysis, including the final determination for how to handle the vulnerability, for any of the 10 vulnerabilities we identified. Also, the State's network devices run on approximately 140 different operating system versions, which can increase the complexity of managing updates and reviewing these security advisories.

This finding represents a material condition because of the importance of managing operating system updates and the weaknesses in DTMB's process for evaluating related security advisories.

RECOMMENDATION

We recommend that DTMB fully establish and implement an effective process for managing updates to the operating systems of network devices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB agrees with the need to establish a formal written process for analyzing security vulnerabilities and updating network devices as necessary. As such, DTMB is formalizing a written internal process and estimates it will be completed in March 2018.

FINDING #4

Network device lifecycle management processes need improvement.

DTMB did not fully establish and implement effective lifecycle management processes to help ensure that only supported network devices (including routers, switches, and firewalls) are operational in the State's IT environment. Unsupported network devices become obsolete and security patches or technical support may no longer be available. This results in an increased risk of network failure, which could negatively impact the availability of the State's critical systems.

According to NIST, organizations should replace information system components when vendor support is no longer available and provide justification and approval for the continued use of unsupported components that are required to satisfy business needs. NIST also states that organizations should implement an enterprise architecture, including the use of roadmaps, to standardize, consolidate, and optimize the use of IT assets. A well-designed enterprise architecture promotes more efficient and cost-effective information security capabilities to help organizations better protect operations and more effectively manage related risks.

SOM Technical Standard 1345.00.82 established the Enterprise Architecture (EA) Technology Roadmaps as the approved list of information technologies endorsed by DTMB for use in the State's IT environment. The roadmaps contain the vendor-designated lifecycle statuses (such as generally available, decline, and end of life) for each device along with the State's planned adoption and obsolescence for each.

Our review disclosed that DTMB did not:

a. Operate only supported network devices in the State's IT environment.

   We reviewed hardware and software version information for 3,876 network devices from DTMB's Orion operational inventory management system. We noted:

   (1) 745 (19%) of the 3,876 devices were no longer supported by the vendor.

   (2) 190 (5%) of the 3,876 devices were running operating systems that were no longer supported by the vendor.

   We were unable to conclude on the lifecycle status for 23 (0.6%) network devices because Orion did not contain sufficient information to base a conclusion. We asked DTMB to identify the hardware and software versions for these 23 devices; however, DTMB did not provide this information.

   DTMB informed us that it evaluated and is planning to replace the majority of these devices as needed.

b. Approve the use of all network devices in operation.

   SOM Technical Standard 1305.00.02 states that any technologies not found on the EA Technology Roadmaps should be reviewed on a case-by-case basis to determine if they are approved for use in the State's IT environment.

   We noted that 1,756 (45%) network devices, covering 73 different vendor model types, were not included on the Network and Telecom Technologies EA Roadmap and had not been formally approved for use in the State's IT environment.

   We were unable to determine if 6 (0.2%) network devices were approved for use and included on the Network and Telecom Technologies EA Roadmap because Orion did not contain sufficient information. We asked DTMB to identify the hardware and software versions for these 6 devices; however, DTMB did not provide this information.

c. Maintain a complete and accurate Network and Telecom Technologies EA Roadmap. Specifically:

   (1) 3 (15%) of the 20 network device hardware series did not have an accurate vendor-designated lifecycle status. As a result, DTMB's designated lifecycle status of these series was incorrect, which could result in obsolete or soon to be obsolete devices being considered approved for use in the State's IT environment.

   (2) 1 (5%) of the 20 network device hardware series did not have an appropriate DTMB-designated lifecycle status. This hardware series was listed as end of life by the vendor but was still considered approved for use in the State's IT environment.

   (3) 4 (100%) of the 4 network device operating systems did not list applicable version numbers. Some of these operating system versions are no longer supported by the vendor. As a result, unsupported operating systems could be considered approved for use in the State's IT environment.

   (4) 1 (5%) of the 20 network device hardware series numbers was inaccurate. The vendor did not manufacture a series with that number. Accurate hardware series information will help DTMB to more effectively and efficiently manage hardware lifecycles.

DTMB informed us that it does not consider the Network and Telecom Technologies EA Roadmap to be the approved listing of network devices and does not use the roadmap to manage the

lifecycle of these devices. Instead, DTMB stated that it relies on an informal process to identify and review new network devices based on the State's future needs. Also, DTMB informed us that it monitors the lifecycle of network devices by reviewing end-of-support notifications and working closely with the vendor. However, DTMB's informal process relies on an incomplete operational inventory which contributed to this finding, as noted in Finding #7.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective lifecycle management processes to help ensure that only supported network devices are operational in the State's IT environment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB is creating an enterprise level asset management capability of network devices. This capability will give us the visibility on devices, warranty periods, and hardware and software end-of-life. Fiscal resources will limit the replacement of unsupported network devices until 2019, but the management process will be in place.

FINDING #5

Security training program improvements needed.

DTMB needs to improve its training program to ensure that individuals responsible for securing the network receive adequate security-related training necessary to perform their assigned duties.

According to Control Objectives for Information and Related Technology* (COBIT), training programs should be developed and delivered to ensure that employees have the knowledge and skills necessary to achieve enterprise goals, including security requirements. SOM Technical Standard 1340.00.030.01 requires that role-based security training be provided annually to personnel with security roles and responsibilities. The Standard also requires that individuals' training records be retained and the effectiveness of the training program be evaluated annually.

Our review disclosed that DTMB had not:

a. Provided training to all individuals with network security roles and responsibilities.

   DTMB informed us that training needs are assessed on an individual basis and may include vendor-specific training, in-house training, and job shadowing as the need arises; however, the training is not always provided to all individuals.

b. Formally evaluated the effectiveness of the training provided.

   According to NIST, organizations should evaluate the effectiveness of training to ensure that it is beneficial and a valuable use of resources. DTMB should evaluate the effectiveness of its security-related training by identifying specific measurable outcomes from the training and assessing whether the outcomes are being achieved.

   DTMB informed us that it holds discussions and monitors performance of staff to evaluate the effectiveness of training.

DTMB was unable to provide historical training records for all staff to demonstrate that staff had received the necessary training and that it was evaluated for effectiveness.

RECOMMENDATION

We recommend that DTMB improve its training program to ensure that individuals responsible for securing the network receive adequate security-related training necessary to perform their assigned duties.

**See glossary at end of report for definition.*

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB will maintain historical training records for individuals with network security roles and responsibilities. DTMB is also establishing a training matrix by skill set and level to track available and required training.

FINDING #6

Procedures need to be more fully developed and implemented.

DTMB did not fully develop and implement comprehensive formal procedures to address a variety of controls for securely managing the network. These procedures would help protect the network from unauthorized access and ensure the availability, confidentiality, and integrity of SOM information.

According to COBIT, management should establish policies to direct the IT control expectations regarding security, confidentiality, and internal control*. COBIT also states that management should establish procedures to maintain compliance with these policies and enforce the consequences of noncompliance.

DTMB Administrative Guide policy 1340.00 adopted NIST Special Publication 800-53 as the minimum security controls for the State's information systems. The policy requires groups responsible for administering information systems to develop and adopt formal documented procedures for implementing and monitoring security controls.

Examples of procedures that DTMB did not develop and implement include:

- Creation, testing, and review of firewall rulesets.
- Configuration management testing and approval process.
- Establishment and periodic review of baseline configurations.
- Lifecycle management of network devices.
- Assignment of privileges and removal and review of user access to network devices.
- Periodic review of inventory completeness and accuracy.
- Vulnerability scans and remediation.
- Monitoring of security events.

DTMB did develop and implement some procedures, such as those related to:

- Installation of a new network device.
- Addition of access to a network device.
- Inventory updates.

** See glossary at end of report for definition.*

- Incident responses for select events.
- Rule management for the SMTP gateway.

The lack of documented procedures contributed to the other findings within this audit report.

RECOMMENDATION

We recommend that DTMB fully develop and implement comprehensive formal procedures to address a variety of controls for securely managing the network.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB will continue to improve on documenting its formal procedures. In addition, DTMB is beginning an IT Policy Process Improvement initiative that will focus on the policy/procedure development process. This initiative is scheduled to be completed in June 2018.

FINDING #7

Complete information needed to track and manage network devices.

DTMB did not ensure that its operational inventory of network devices contained complete information, which may negatively impact the effectiveness and efficiency of DTMB's security management operations.

We reviewed Orion and determined that:

a. 296 (8%) of 3,876 device records did not contain the device type.

b. 148 (4%) of 3,876 device records did not contain an operating system version.

c. 6 (0.2%) of 3,876 device records did not contain the vendor name.

d. 6 (0.2%) of 3,876 device records did not contain a system description.

According to NIST, organizations should develop, document, and maintain an inventory that accurately reflects current information systems at a level of granularity deemed necessary for proper tracking and reporting. The accuracy of this information should be maintained through periodic manual inventory checks or a network monitoring tool that automatically maintains the inventory. DTMB utilizes Orion to manage the majority of the State's production network devices.

DTMB informed us that custom fields within Orion require manual entry and other fields are automatically populated using information obtained from the network device.

We determined that the lack of complete information in the operational inventory contributed to the weaknesses noted in Finding #4.

RECOMMENDATION

We recommend that DTMB ensure that its operational inventory of network devices contains complete information.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees with the recommendation. DTMB is consolidating its various asset management capabilities into an enterprise level operational inventory of network devices.

SECURITY AND ACCESS CONTROLS

BACKGROUND

In the event that an IT network is compromised, connected IT assets could be at risk. Ensuring that network devices are securely configured is a key factor in ensuring the security of the State's network and data.

Access controls* limit or detect inappropriate access to network resources, thereby protecting them from unauthorized modification, loss, and disclosure.

NTSD is responsible for configuring the State's network devices such as routers, switches, and firewalls. Technical Services handles configuration for network devices within the State's Next Generation Digital Infrastructure (NGDI) environment.

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's security and access controls over the State's IT network.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB implemented some firewall controls and network device security configurations in accordance with State policy and industry best practices.
- One material condition related to establishing and implementing effective controls over the management of firewalls (Finding #8).
- Two reportable conditions related to improving the configuration of network device operating systems and establishing and implementing effective administrative access controls over the State's network devices (Findings #9 and #10).

** See glossary at end of report for definition.*

FINDING #8

Controls over firewalls need to be improved to ensure security of the network.

DTMB did not establish and implement effective controls over the management of firewalls to help protect the State's network from threats.

According to NIST, firewalls provide a layer of security that allows organizations to prevent unauthorized access to their systems and resources. NIST states that management of firewalls is critical to achieving protection of network traffic.

Our review disclosed that DTMB did not:

a. Periodically review firewall rulesets to ensure that each rule is required to be operational and is in compliance with security requirements.

   NIST recommends that organizations review firewall rulesets often to identify rules that are no longer needed as well as new policy requirements that should be added to the firewall.

b. Review all changes to firewall rulesets.

   NIST states that organizations should perform a detailed examination of all changes since the last regular review, particularly who made the changes and under what circumstances.

   DTMB standard requires that changes made to firewall rules follow a formal change management process whereby MCS reviews and approves change requests, which are then implemented by NTSD. MCS informed us that it reviews certain firewall rulesets for changes. However, MCS should actively monitor all changes made to firewall rulesets to ensure that the formal change management process is followed and that the changes were appropriate.

Periodic testing of firewall rulesets needed.

c. Periodically test firewall rulesets to ensure that rules are functioning as intended.

   According to NIST, an important task for managing firewalls is to perform periodic testing to verify that firewall rules are functioning as expected.

   DTMB informed us that it tests firewall rules only when a rule is implemented. Testing does not always take into account the entire ruleset and is not done on a periodic basis.

d. Ensure that rulesets were configured in full compliance with DTMB standards or industry best practice recommendations.

   NIST states that organizations should configure firewall rulesets as defined in the system security plan to control

network traffic in the most restrictive way possible. SOM Technical Standard 1345.00.09 outlines the State's security requirements for configuring firewall rulesets.

We determined that 12 (86%) of 14 randomly sampled rulesets were not in compliance with DTMB standards or industry best practices. Because of the confidentiality of these rulesets, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

e. Fully document the review and approval of changes to firewall rulesets.

SOM Technical Standard 1345.00.09 requires that a DTMB-0090 form and remedy change request be completed, reviewed, and approved prior to implementing a firewall rule change.

Our review of a random sample of 48 firewall rule changes disclosed:

(1) 6 (13%) did not have an associated DTMB-0090 form.

Several firewall ruleset changes were not documented, reviewed, and approved.

(2) 5 (10%) did not have an associated remedy change request.

(3) 12 (29%) of the 42 DTMB-0090 forms did not contain accurate technical information on the rule.

(4) 9 (21%) of the 43 remedy change requests did not document that testing was performed prior to implementation of the rule.

(5) 8 (19%) of the 43 remedy change requests did not indicate that the IT asset mentioned in the rule change passed a vulnerability scan prior to implementation of the rule.

(6) 3 (7%) of the 43 remedy change requests did not contain proper approvals.

f. Ensure that all firewalls were monitored with the State's firewall management tool.

NIST states that, when tools are available within an organization to monitor firewalls, they should be used periodically as part of a regular review.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of firewalls in securing the State's network.

RECOMMENDATION

We recommend that DTMB establish and implement effective controls over the management of firewalls to help protect the State's network from threats.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB will continue to improve the documentation, review, and approval of firewall rulesets in accordance with its effective controls in managing firewalls. Since February 2015, DTMB implemented a more structured automated audit process to help ensure firewall rules were implemented in compliance with State standards. DTMB continues to use this process for all new firewall rules. As DTMB expands its NGDI environment, older firewall rules will be decommissioned. DTMB is evaluating additional opportunities to further automate and control the compliance with the State's firewall rule standards.

FINDING #9

Improvements in network device configurations needed.

DTMB did not configure network device operating systems in accordance with best practices. Proper configuration reduces the risk of compromise to the State's information systems and data, thereby protecting them from unauthorized modification, loss, or disclosure.

According to NIST, the configuration of an information system and its components has a direct impact on the security posture of the system. Network device manufacturers provide configuration recommendations on how to secure their devices to increase the overall security of the network. DTMB should apply best practice configurations to network device operating systems to reduce the number of vulnerabilities that attackers can attempt to exploit and lessen the impact of successful attacks.

We reviewed network device operating system configuration settings for a sample of 45 network devices. We noted deviations from vendor hardening guides and DTMB standards on 45 (100%) of 45 network devices, ranging from 6 to 26 deviations per each device. Because of the confidentiality of those configurations, we summarized our testing results for presentation in this finding and provided the detailed results to DTMB management.

We noted that DTMB had not fully established and implemented effective configuration management controls in Finding #1, which we determined contributed to the deficiencies within this finding. Effective configuration management controls are important for establishing and maintaining secure network device configurations.

RECOMMENDATION

We recommend that DTMB configure network device operating systems in accordance with best practices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB has remediated 96% of the baseline configuration exceptions that DTMB agrees with. The remaining issues will require further assessment and extra coordination and are, therefore, longer-term remediations.

FINDING #10

Improved controls over administrative access would help reduce the risk of unauthorized access.

DTMB did not fully establish and implement effective administrative access controls over the State's network devices. Protecting access to network devices helps prevent unauthorized users from making configuration changes that could disrupt the stability and compromise the security of the network.

SOM policy 1335.00 establishes the protection of information and systems against unauthorized access to or modification of information. The policy requires that access be controlled using authentication, authorization, and accountability.

We reviewed administrative access to a sample of 45 network devices for compliance with DTMB standards and industry best practices. We noted:

a. Administrative user accounts had inappropriate access. Specifically:

   (1) 5 accounts that remained active after the user left State employment.

   (2) 4 users with access beyond what was required to perform their job responsibilities.

   (3) 1 user with multiple accounts. Because of an employment change, the user was generated a second account. Upon creation of the new account, the old account should have been removed.

   SOM Technical Standard 1340.00.020.01 requires that DTMB implement the concept of least privilege.

b. For 11 (79%) of 14 users reviewed, DTMB was unable to provide evidence of management approval of the access rights granted to network device administrators.

   SOM Technical Standard 1340.00.020.01 requires approvals by DTMB authorized requestors or other appropriate personnel for the creation of accounts. Approval should specify the authorized user, role membership, and authorized access rights.

c. Recertification of user access rights was not sufficiently documented. DTMB implemented a process to generate listings every two months of users with network device access; however, documentation of management's review of the appropriateness of continued access was not available.

   SOM Technical Standard 1340.00.020.01 requires that accounts be reviewed for compliance with account management requirements every 120 days.

d. Three (7%) of 45 devices reviewed allowed users to make configuration changes without using the State's multifactor solution as required by SOM Technical Standard 1340.00.03.

e. For 2 (4%) of the 45 devices reviewed, administrators configured the device through a single shared account, instead of using a unique account as required by SOM Technical Standard 1340.00.03.

DTMB informed us that it has been working on improvements to access controls; however, these improvements had not been fully completed at the time of our audit.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective administrative access controls over the State's network devices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. During the course of the audit, DTMB executed many user access corrections on the spot. DTMB has processes in place to control administrator access and will continue to improve the documentation of the process.

MONITORING OF NETWORK SECURITY

BACKGROUND

Achieving adequate information security for an organization is a multifaceted undertaking that requires continuous monitoring of the organization and its information systems to determine the effectiveness of deployed security controls and ensure compliance with standards.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to monitor the security of the State's IT network.

CONCLUSION

Moderately sufficient.

FACTORS IMPACTING CONCLUSION

- DTMB has conducted some penetration testing to assess the risk and threats facing the network.
- DTMB has implemented or started implementing tools for conducting vulnerability scans and monitoring security events.
- One material condition related to establishing and implementing effective risk management practices over the State's IT network (Finding #11).
- Two reportable conditions related to monitoring high risk network security events and securing access to network monitoring tools and implementing an effective monitoring process for unauthorized wireless access points (Findings #12 and #13).

FINDING #11

DTMB did not fully establish and implement effective risk management practices over the State's IT network to help ensure that security risks are identified and sufficiently evaluated.

Risk management practices not fully established and implemented.

COBIT states that organizations should evaluate and approve IT risk tolerance thresholds, evaluate risk factors, and establish management practices to ensure that actual IT risk does not exceed acceptable levels.

Our review of DTMB's risk management practices disclosed:

a. DTMB did not conduct a risk assessment* of the network.

   SOM Technical Standard 1340.00.150.01 requires that, at least annually, a risk assessment be conducted including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the data that the systems process, store, and transmit.

b. DTMB did not fully implement an effective process for identifying and remediating vulnerabilities on network devices. Vulnerability management is critical to ensuring that network security threats are identified and remediated before they can be exploited.

   SOM Technical Standard 1340.00.150.01 requires that processes be implemented for vulnerability scanning, evaluation of identified vulnerabilities, and remediation of legitimate vulnerabilities.

   DTMB has access to a third-party vulnerability management tool to conduct scans of network devices. These scans identify known and potential vulnerabilities in the configuration of the device. The tool provides a score indicating the severity of the vulnerability as well as remediation information.

   Our review of scan and vulnerability histories for 45 sampled network devices disclosed that DTMB did not:

   (1) Conduct authenticated vulnerability scans for 45 (100%) of the 45 devices.

   Authenticated and unauthenticated vulnerability scans not conducted on 45 and 39, respectively, of the 45 sampled devices.

   SOM Technical Standard 1340.00.150.01 requires that DTMB perform authenticated vulnerability scans for all network devices at least every 30 days. An authenticated scan allows for a more in-depth security assessment and better visibility into each network device's security posture. DTMB informed us that its third-party vulnerability management tool has not been configured to allow for authenticated scans.

** See glossary at end of report for definition.*

(2) Conduct unauthenticated vulnerability scans for 39 (87%) of the 45 devices.

DTMB's vulnerability management tool has the ability to complete less robust unauthenticated scans. DTMB informed us that only network devices with specific compliance requirements are subject to vulnerability scanning even though SOM Technical Standard 1340.00.150.01 requires that all devices be scanned.

(3) Timely identify or remediate high and medium severity vulnerabilities.

SOM Technical Standard 1340.00.150.01 requires that all network devices be scanned every 30 days. High and medium severity vulnerabilities must be remediated within 30 and 60 days, respectively. If remediation cannot be completed in the required time frame, compensating controls must be put in place and the DTMB exception process must be followed.

Our review of 6 devices that had received a vulnerability scan during our audit period disclosed:

(a) Monthly scanning for 1 (17%) device had not been implemented.

(b) 13 (68%) of 19 high severity vulnerabilities had not been remediated.

(c) 33 (55%) of 60 medium severity vulnerabilities had not been remediated.

(d) 5 (83%) of the 6 remediated high severity vulnerabilities were not remediated within 30 days.

(e) 12 (44%) of the 27 remediated medium severity vulnerabilities were not remediated within 60 days.

In addition, we requested that DTMB perform an unauthenticated vulnerability scan for our 45 sampled network devices as of August 15, 2017.

The unauthenticated scan results disclosed a significant number of vulnerabilities, supporting the need for regular scans:

Severity Level of Vulnerability	Number of Vulnerabilities Identified
High	82
Medium	167

c. DTMB should further its penetration testing efforts.

According to NIST, penetration testing is a specialized assessment to identify vulnerabilities that could be exploited. Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides an in-depth analysis of security-related weaknesses.

DTMB contracted with a vendor in 2015 to perform penetration testing on selected network components. Conducting additional penetration tests with differing scopes and methodologies will further allow DTMB to understand the risks facing the network and protect it from cyber security threats. DTMB informed us that it plans to conduct penetration testing throughout the five-year contract with the vendor.

We consider this finding to be a material condition because of the lack of risk assessments, number of vulnerabilities not identified and remediated by DTMB, and the impact these vulnerabilities have on the security posture of the network.

RECOMMENDATION

We recommend that DTMB fully establish and implement effective risk management practices over the State's IT network to help ensure that security risks are identified and sufficiently evaluated.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation.

Since October 2017, the State CIO is implementing an effective risk management framework adopted from Federal agencies in accordance with NIST guidelines. The Security Accreditation Process of systems/applications is based on standardized architecture and NIST controls and will result in Authority to Operate (ATO) certifications for each system/application. Each ATO will have Security Accreditation Plans that document system information and security requirements and related controls for systems/applications and Plans of Actions and Milestones (POAMs) for the associated risks. Signature by the business owners and the State CIO will indicate acceptance of the documented risk and mitigation measures.

Additionally, DTMB performs monthly vulnerability scanning of the State's border protection and core devices, which helps ensure critical data infrastructure is protected. Most potential attacks are stopped at the enterprise border protection devices. Using a risk-based approach, DTMB will continue to evaluate improvements to the scanning process.

FINDING #12

Improvements needed over network monitoring.

DTMB did not monitor all high risk network security events and did not always properly secure access to network monitoring tools to help protect against threats and improve the security of the network.

NIST Special Publication 800-53 defines an information system event as any observable action within an information system. Security events are the events that an organization has identified as significant and relevant to the security of the information system and the environment in which it operates.

Our review of DTMB's network monitoring processes disclosed that DTMB did not:

a. Conduct a formal assessment to determine which security risks and events should be monitored.

   SOM Technical Standard 1340.00.040.01 requires that DTMB determine the events to be monitored based on current threat information and an ongoing assessment of risk.

   DTMB informed us that it implemented an enterprise security correlation tool for monitoring security events. Also, DTMB informed us that, for other monitoring tools, it relies on subject matter experts to determine which events should be monitored. However, DTMB did not explicitly identify the security events to be monitored for the State's network environment and did not formally periodically assess that the events being monitored are appropriate.

b. Document its remediation efforts for those security events that were monitored.

   SOM Technical Standard 1340.00.040.01 requires that audit records be reviewed and analyzed at least weekly.

   DTMB informed us that its analysis and follow-up on security events were documented when remediation was required. However, DTMB was unable to produce documentation to support its review.

c. Maintain documentation to support that it followed the official change management process for the creation of SMTP gateway incoming mail rules.

   According to NIST Special Publication 800-45, to ensure security of the mail gateway, a change management process should be followed for all configuration changes.

   DTMB was unable to produce change management documentation showing authorization for the creation of 6 (75%) of 8 selected SMTP gateway rules.

d. Fully secure access to network monitoring tools.

SOM Technical Standard 1340.00.040.01 requires that audit information and audit tools be protected from unauthorized access, modification, and deletion.

We noted:

(1) 4 user accounts remained active after the users were no longer employed by the State.

(2) 8 user accounts remained active after the users had not logged on in more than 60 days, indicating that access was not required for the users' regular job functions.

(3) 1 administrative account could be accessed by multiple users and was used to perform nonadministrative level job functions.

(4) 1 monitoring tool did not require multifactor authentication and did not enforce an adequate password policy.

RECOMMENDATION

We recommend that DTMB monitor all high risk network security events and properly secure access to network monitoring tools to help protect against threats and improve the security of the network.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB performs event correlation monitoring, which is a sophisticated level of monitoring. DTMB's Security Information and Event Management (SIEM) system aggregates and consolidates information from 1,800 different log sources to identify, correlate, and analyze security events. The State's SIEM allows for an effective approach to analyze security events against these different log sources. This approach allows the State to automatically support incident handling by centralized initiation of these security events.

DTMB also subscribes to services provided by the State's Internet Service Providers to monitor denial-of-services events. If a denial-of-service event happens, DTMB is notified of the event and takes appropriate action. DTMB correlates information from various sources to determine if a security event has occurred. DTMB continually refines the process to identify the security risks and events to be monitored.

During the course of the audit, DTMB executed many user access corrections on the spot. DTMB has processes in place to control administrator access to monitoring tools and will continue to improve documentation of the process.

FINDING #13

DTMB did not fully implement an effective monitoring process to ensure that the State's IT network is protected against the threats presented by unauthorized wireless access points.

Monitoring process for unauthorized wireless access points needs to be fully implemented.

NIST Special Publication 800-153 recommends that organizations monitor for unauthorized wireless access points which could disrupt wireless LAN operations through denial-of-service attacks, resulting in legitimate clients being unable to access SOM wireless LAN resources. In addition, malicious third parties could attempt to capture sensitive information from clients that connect to an unauthorized wireless access point. Organizations should utilize automated detection tools and implement monitoring processes to investigate unauthorized wireless access points in their wireless air space to minimize these risks.

Although DTMB purchased an enterprise solution to identify and investigate unauthorized wireless access points, it did not formally assign responsibility for monitoring those access points. While event logs are continuously generated, DTMB does not regularly monitor the logs to detect and investigate unauthorized wireless access points. For the month of May 2017, approximately 79,000 log entries were generated from DTMB's enterprise solution.

RECOMMENDATION

We recommend that DTMB fully implement an effective monitoring process to ensure that the State's IT network is protected against the threats presented by unauthorized wireless access points.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with this recommendation. DTMB configures and manages all of its wireless access points to require network authentication by only authorized devices before connecting them to the SOM network. DTMB monitors the wireless network, and detects thousands of requests from unauthorized devices which are summarily denied.

Improving the issues noted in Finding #2 will prevent rogue access point risks.

CYBER SECURITY AWARENESS PROGRAMS

BACKGROUND

Cyber security is the practice of defending an organization's network, computers, and data from unauthorized access, attack, or damage by implementing secure processes and technologies. Weaknesses in an organization's cyber security can lead to disruption of critical business processes, degradation of business performance, increase in security costs related to remediation, and breach of confidential or sensitive data. Cyber security threats include but are not limited to phishing*, malware, viruses, zero-day exploits, and social engineering.

Within DTMB, MCS is responsible for increasing levels of security awareness, providing security and technology related training opportunities, and sponsoring enterprise-wide security education events.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's cyber security awareness programs.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Survey responses of 4,459 State executive branch employees generally indicated a sufficient level of awareness of cyber security threats and an understanding of the State's security practices.
- One reportable condition related to continuing necessary cyber security awareness training (Finding #14).

** See glossary at end of report for definition.*

FINDING #14

Security awareness training program should continue.

DTMB should continue its cyber security awareness training program to help ensure that information system users maintain a secure environment and respond to cyber security threats appropriately.

Cyber security awareness training is a formal process for educating users about security and IT policies and procedures. DTMB Technical Standard 1340.00.030.01 requires that security awareness training be provided to information system users. The Standard also requires that an evaluation of the effectiveness of this training be performed on a yearly basis.

DTMB contracted with a vendor to develop the State's cyber security awareness training program, which consisted of 24 interactive lessons delivered every two months. Our review of the training program disclosed that DTMB did not:

a. Formally assess the effectiveness of its cyber security awareness training.

   According to NIST, evaluating effectiveness is a vital step in ensuring that training is cost effective and satisfies the organizational needs. Evaluating the effectiveness of training should include activities such as:

   - Identifying how useful the participants found the training.
   - Determining if participants improved their cyber security knowledge and skills.
   - Assessing the extent of which participants changed their behavior.
   - Assessing the measurable benefits achieved as a result of the training.

   DTMB should consider performing the following activities to assess the effectiveness of its cyber security awareness training:

   - Conduct phishing exercises to measure the success of lessons related to phishing.
   - Evaluate how the training impacts the number and type of cyber incidents occurring.
   - Test the participants' knowledge of the training topics and evaluate the results in order to assess delivery of the content.

   DTMB informed us that, after the lesson on the topic of phishing, it noticed an increase in the number of security incidents reported to its security tips mailbox. However, a formal evaluation would help DTMB assess the awareness

of each user, make any necessary changes to the training, and more effectively manage the State's cyber security risk.

b. Ensure satisfactory participation rates in the cyber security awareness training.

DTMB set a goal of 85% employee participation in the training program. We noted that an average of 68% of State employees participated in each of the 24 training lessons, as follows:

Title of Lesson	Number of Employees Completing Lesson	Number of Employees Enrolled in Training Program	Percentage of Employees Completing Lesson
Intro to Security Awareness	44,468	60,212	74%
Office Security	44,171	60,212	73%
Computer Security	43,980	60,212	73%
Passwords	43,711	60,212	73%
Email Security	43,385	60,212	72%
Web Security	42,867	60,212	71%
Phishing	42,531	60,212	71%
Information Protection	42,069	60,212	70%
Mobile Security	41,669	60,212	69%
Social Networking	41,215	60,212	68%
Public WiFi	40,601	60,212	67%
Incident Reporting	39,700	60,212	66%
Safe Disposal	40,224	60,212	67%
Travel Security	39,574	60,212	66%
Social Engineering	39,129	60,210	65%
Privacy	38,276	60,210	64%
Working Remotely	37,111	60,207	62%
Data Loss Prevention	34,477	60,202	57%
Phishing	42,907	59,405	72%
Social Engineering	42,103	58,754	72%
Insider Threat	41,395	58,331	71%
Information Protection	40,038	57,704	69%
Internet of Things	38,518	57,235	67%
Cloud Security	30,261	56,407	54%
Average	40,599	59,651	68%

DTMB informed us that its contract with the vendor prevented some employees who hired after the program started from accessing historical lessons, which impacted the participation rates. DTMB also informed us that it highly encouraged all State executive branch departments to participate in the training and that some made a decision not to require the training for all of its employees.

It is vital to the State's network security that employees participate in a complete cyber security awareness training program to fully understand cyber security threats and learn how to protect confidential information, including the

consequences of their actions. DTMB has authority to enforce participation in the training through Executive Order No. 2009-55, which requires DTMB to identify and implement security best practices and standards throughout State government and develop and implement processes to replicate IT best practices and standards throughout the executive branch. However, DTMB did not use its executive authority to enforce participation in the training.

To further evaluate the effectiveness of DTMB's cyber security awareness training program, we conducted a phishing exercise on a random sample of 5,000 State employees from 18 executive branch departments and the Executive Office. A phishing attack is a cyber security threat used to deceive an e-mail recipient by posing as a legitimate entity. Our exercise involved sending an e-mail to employees requesting them to click on a link and enter their credentials. The following table summarizes the results of the exercise:

	Number of Employees	Percentage of Employees
Opened the e-mail	1,619	32%
Clicked the link within the e-mail	1,238	25%
Entered credentials	945	19%

There are many potential threats of phishing attacks. According to the SANS Institute, the potential consequences from being phished include identify theft, unauthorized use of accounts, stolen information, and damage to credibility, all which may take years for an organization to fully recover. DTMB informed us that the e-mail from our exercise was reported to its security tips mailbox multiple times and that other controls are in place which may limit the effectiveness of these types of attacks.

RECOMMENDATIONS

We recommend that DTMB continue its cyber security awareness training program to help ensure that information system users maintain a secure environment and respond to cyber security threats appropriately.

We also recommend that DTMB take steps to ensure that all information system users participate in its cyber security awareness training program.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendations. DTMB continually improves its security awareness and training program. In August 2017, DTMB implemented Version 2.0 of its cyber security awareness training program. It includes a mechanism to assess the effectiveness of the program.

DTMB will continue to evaluate user participation in its security awareness program and begin to tie users' continued access to the network to their trends in participation in the program.

DESCRIPTION

Network security refers to any activity designed to protect the availability, confidentiality, and integrity of a network and data. It includes the implementation of hardware and software technologies to help secure the network. Cyber security is the practice of defending an organization's network, computers, and data from unauthorized access, attack, or damage by implementing secure processes and technologies.

Within DTMB, network and cyber security are primarily the responsibility of NTSD, MCS, Design & Delivery, and Technical Services:

- NTSD's mission is to provide highly efficient and cost-effective managed network services to all SOM agencies and their clients. Some of NTSD's primary responsibilities include design, configuration, and maintenance of network devices such as routers, switches, and firewalls.

- MCS is responsible for providing oversight, cyber security awareness training, and enforcement of enterprise-wide network security. MCS also manages some of the tools used to monitor network security with the goal of eliminating or reducing cyber security threats.

- Design & Delivery, in conjunction with MCS, manages the State's SMTP gateway. Responsibilities of managing the gateway include monitoring inbound e-mail and blocking potential malicious attacks before they reach a State employee's mailbox.

- Technical Services manages the State's private cloud service, NGDI, including design, configuration, and maintenance of network devices specific to that environment.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the IT records of the State's network and cyber security. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit scope did not include physical location inventory controls over network devices, which were included in the scope of our performance audit of Physical Security and Environmental Controls Over Information Technology Resources issued in December 2015.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2014 through September 30, 2017.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of the State's network and cyber security to formulate a basis for defining our audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed management and staff responsible for administering network and cyber security.
- Reviewed DTMB policies, standards, and procedures for configuring and securing the State's network.
- Obtained an understanding of the areas responsible for network and cyber security within DTMB.
- Obtained an understanding of network monitoring tools.

OBJECTIVE #1

To assess the sufficiency of DTMB's efforts to design and administer a secure IT network.

To accomplish this objective, we:

- Compared established policies, standards, and procedures governing network administration and design with industry best practices.

** See glossary at end of report for definition.*

- Reviewed training records for staff with security roles and responsibilities.
- Reviewed the Orion operational inventory for completeness.
- Assessed lifecycle status of 3,876 network devices in operation.
- Evaluated network diagrams for conformity with the device inventory and compliance with industry best practices.
- Reviewed network segmentation and design for compliance with industry best practices.
- Evaluated availability metrics for the network.
- Assessed DTMB's network device access control and network discovery processes.

Our testing population generally consisted of State-owned routers, switches, and firewalls.

OBJECTIVE #2

To assess the effectiveness of DTMB's security and access controls over the State's IT network.

To accomplish this objective, we:

- Tested configuration settings for a random sample of 45 network devices for compliance with DTMB standards and vendor hardening guides.
- Reviewed access controls for a random sample of 45 network devices.
- Assessed the network device update management process.
- Evaluated a random sample of 14 firewall rulesets and 48 corresponding rules for compliance with DTMB standards and industry best practices related to configuration, monitoring, testing, and change management processes.

Our testing population for this objective consisted of 3,126 network devices, generally consisting of State-owned routers, switches, and firewalls. This population was limited to devices still supported by the vendor and, as a result, excluded end-of-life devices reviewed under Objective #1.

OBJECTIVE #3

To assess the sufficiency of DTMB's efforts to monitor the security of the State's IT network.

To accomplish this objective, we:

- Reviewed DTMB's processes for monitoring security events and controlling access to monitoring tools.
- Evaluated network risk assessments, penetration tests, and vulnerability scan and remediation efforts.
- Assessed processes for monitoring unauthorized wireless access points.

OBJECTIVE #4

To assess the effectiveness of DTMB's cyber security awareness programs.

To accomplish this objective, we:

- Surveyed 12,500 State executive branch employees and evaluated the 4,459 responses received to assess the level of awareness of cyber security threats and the understanding of the State's security practices.
- Reviewed the participation rates and effectiveness of DTMB's cyber security awareness training program.
- Performed a phishing exercise on a random sample of 5,000 State executive branch employees.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions or reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality of network device configurations, diagrams, and other data, we summarized portions of our testing results for presentation in the report and provided the underlying details to DTMB management.

AGENCY RESPONSES

Our audit report contains 14 findings and 15 corresponding recommendations. DTMB's preliminary response indicates that it agrees with 12 of the recommendations and partially agrees with 3 of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our

fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
baseline configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
CIO	chief information officer.
configuration	The set of parameters that can be changed within hardware, software, or firmware that affect the security posture and/or functionality of the information system.
configuration checklist	Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific IT platforms/products and instructions for configuring those information system components to meet operational requirements.
configuration management	The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over IT.
DTMB	Department of Technology, Management, and Budget.
EA	Enterprise Architecture.
effectiveness	Success in achieving mission and goals.
event	Any observable occurrence in an information system.
firewall	Hardware and software components that protect one set of system resources (e.g., computers or networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to

	access and transmit privileged information and deny access to unauthorized users.
internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.
IP	Internet Protocol.
IT	information technology.
LAN	local area network.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
MCS	Michigan Cyber Security.
NAC	network access control.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
NGDI	Next Generation Digital Infrastructure.
NTSD	Network and Telecommunication Services Division.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

phishing	Attacks perpetrated by criminals who send deceptive e-mails to lure someone into visiting a fraudulent Web site or downloading malicious software to steal sensitive information, such as credit card numbers, account information, and passwords.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
risk assessment	The process of identifying risks to entity operations (including mission, functions, image, or reputation), entity assets, or persons by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
SANS Institute	A research and education organization that develops, maintains, and makes available at no cost research documents about various aspects of information security. The SANS Institute also offers computer security training and certification.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
SMTP	Simple Mail Transfer Protocol.
SOM	State of Michigan.
threat	Any circumstance or event with the potential to cause adverse impact through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat. Examples include injection vulnerabilities, buffer overflows, or privilege escalation.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650