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