Office of the Auditor General
Performance Audit Report

Physical Security and Environmental Controls Over Information Technology Resources

Department of Technology, Management, and Budget

December 2015

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

071-0500-15

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

Physical Security and Environmental Controls Over Information Technology Resources

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0500-15

Released:
December 2015

DTMB's Data Center Operations (DCO) maintains and secures the State's three hosting centers that house computer servers containing the State's automated information systems. DTMB's Network and Telecommunications Services Division maintains and secures the State's computer network equipment that transmits data to and from the hosting centers. Network equipment is stored in switch rooms and telecommunication rooms located throughout the State.

Audit Objective	Conclusion
Objective #1: To assess the adequacy of DTMB's physical security controls in place at locations housing the State's information technology (IT) resources.	Generally adequate

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not fully implement controls to limit physical access to the State's telecommunication equipment to only those individuals requiring access. Rooms housing telecommunication equipment were not always secured (Finding #1).	X		Agrees
DTMB did not establish adequate physical security in and around the hosting centers and switch rooms. Former employees still had access to hosting centers and switch rooms (Finding #2).		X	Agrees
DTMB did not maintain complete and accurate records of the State's telecommunication equipment. Some new equipment purchases were not added to inventory systems (Finding #3).		X	Agrees

Audit Objective	Conclusion
Objective #2: To assess the adequacy of DTMB's environmental controls in place at locations housing the State's IT resources.	Generally adequate

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not implemented adequate environmental controls over IT equipment located throughout the State. Some rooms were not reasonably free from dust, food and beverages, or general storage items. Also, water and fire hazards existed in some locations (Finding #4).	X		Agrees

Audit Objective	Conclusion
Objective #3: To assess the effectiveness of DTMB's governance over physical security and environmental controls at locations housing the State's IT resources.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not prepared and approved plans for the replacement of mechanical equipment that has exceeded its life expectancy. Air conditioning units in the switch rooms were 5 to 12 years beyond their manufacturers' expected life with no plan for replacement (Finding #5).		X	Agrees
DTMB did not maintain documentation to support the completion of the required preventive maintenance services for the transient voltage surge suppressor units. Preventive maintenance helps ensure that equipment is functioning properly and not in need of repair or replacement (Finding #6).		X	Agrees

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: www.audgen.michigan.gov

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

OAG
Office of the Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • www.audgen.michigan.gov

Doug A. Ringler, CPA, CIA
Auditor General

December 18, 2015

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

Dear Mr. Behen:

I am pleased to provide this performance audit report on the Physical Security and Environmental Controls Over Information Technology Resources, 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 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

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS OVER INFORMATION TECHNOLOGY RESOURCES

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

IMPLEMENTING PHYSICAL SECURITY CONTROLS

BACKGROUND

Physical security controls* restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Examples of physical security controls include the use and control of identification badges, exterior lighting, fencing around buildings, cameras to monitor the building perimeter, locked doors, and security guards. Poor physical security controls can result in unauthorized access, damage, or theft of resources located within the computer facility.

The Department of Technology, Management, and Budget's (DTMB's) Data Center Operations (DCO) and Network and Telecommunications Services Division (NTSD) manage physical security of the hosting centers*, switch rooms*, and rooms containing telecommunication equipment.

The Federal Information System Controls Audit Manual* (FISCAM) is an industry standard in security controls.

AUDIT OBJECTIVE

To assess the adequacy of DTMB's physical security controls in place at locations housing the State's information technology* (IT) resources.

CONCLUSION

Generally adequate*.

FACTORS IMPACTING CONCLUSION

- Establishment and implementation of several physical security controls at the hosting centers and switch rooms.
- Compensating controls, such as surveillance camera in place to reduce the risk of unauthorized access to the hosting centers.
- Physical security controls in place at the State's IT equipment storage warehouse.
- Establishment and implementation of some physical security procedures over rooms housing telecommunication equipment.
- Inventory controls implemented for servers and other equipment located in the hosting centers.

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

- Material condition* related to physical security of the State's IT resources, primarily related to telecommunication equipment, and reportable conditions* related to physical security in and around the State's hosting centers and switch rooms and inventory controls for telecommunication equipment.

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

FINDING #1

Improved physical security controls are needed to protect the State's telecommunication equipment.

DTMB did not fully implement controls to limit physical access to the State's telecommunication equipment to only those individuals requiring access, which may lead to the State's IT resources being stolen or damaged.

FISCAM states that physical security controls should be established to secure the perimeter of a computer facility and to control access into and within the facility. Computer resources that should be physically protected include the primary computer rooms; telecommunication equipment, such as switches and routers; and transmission lines.

Our review of physical security at 163 main telecommunication rooms* (MTRs) and telecommunication rooms* (TRs) located within 83 of the approximately 790 State office buildings throughout Michigan disclosed:

a. Rooms containing telecommunication equipment had physical security vulnerabilities. Because of the confidentiality of the vulnerabilities, we separately provided the detailed results to DTMB management.

b. NTSD did not ensure that telecommunication equipment was located in designated MTRs and TRs. Telecommunication equipment was located in garages, break rooms, and general office areas in 12 (7%) of the 163 rooms we visited. DTMB Technical Standard 1345.00.02 requires that an MTR be located in each building and that each floor of the building contain at least one TR.

Rooms housing telecommunication equipment were not always secured.

c. NTSD did not ensure that doors to the MTRs and TRs were secured. As noted in part b., 12 of the 163 rooms containing telecommunication equipment were not designated MTRs or TRs and did not have doors. Of the remaining 151 MTRs and TRs, we noted:

   (1) Door hinges for 13 (9%) MTRs and TRs had removable pins or were not installed with the pins on the inside of the room as required by DTMB Technical Standard 1345.00.02.

   (2) Doors for 80 (53%) MTRs and TRs did not swing outward as required by DTMB Technical Standard 1345.00.02. In one building, the TR door opened into and hit the telecommunication equipment.

DCO and NTSD agreed that the exceptions noted in this finding were the result of not following DTMB policies when the equipment was installed. NTSD did not always have control over the space where the telecommunication

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

equipment was installed, particularly in leased buildings, which contributed to the exceptions noted in parts a., b., and c. In addition, some exceptions in part a. resulted from lack of policy and insufficient training on the importance of keeping these rooms secure.

RECOMMENDATION

We recommend that DTMB fully implement controls to limit physical access to the State's telecommunication equipment to only those individuals requiring access.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB has already restricted access to only those individuals who require access and will review card key access reports every six months. DTMB will evaluate the location of all telecommunication equipment and, where possible, isolate the equipment in an MTR/TR. In addition, DTMB will evaluate possible solutions to ensure that MTR/TR doors are secure and will evaluate how to best improve physical security controls over MTRs/TRs in leased buildings.

FINDING #2

Improved physical security is needed in and around hosting centers and switch rooms.

DTMB did not establish adequate physical security in and around the State's hosting centers and switch rooms, which could lead to unauthorized individuals gaining access to the hosting centers, damaged equipment, improper data access, and disruption of services.

FISCAM states that adequate physical security controls should be established commensurate with the risks of physical damage or access and include securing the perimeter of the facility and controlling access into and within a computer facility. Computer resources to be protected include primary computer facilities; network devices, such as routers and firewalls; and telecommunication equipment and transmission lines.

Our review of physical security controls at DTMB's 3 hosting centers and 8 DTMB-managed switch rooms disclosed:

Former employees still had access to the State's hosting centers and switch rooms.

a. DTMB did not adequately review the list of persons with access to the hosting centers and switch rooms to identify and remove persons no longer requiring access. Our review of access to the 2 primary hosting centers and 8 switch rooms disclosed former employees who still had access and employees without background checks on record as follows:

	Individuals With Access	Former Employees With Access	Individuals With Access Without Background Check
Hosting Center 1	45	5 (11%)	5 (11%)
Hosting Center 2	43	6 (14%)	4 (9%)
Switch Rooms	98	4 (4%)	Not applicable

DTMB procedure HCSPRO-0001, Data Center Operations, states that DTMB will grant access to secured facilities to only those individuals whose primary daily duties require work within the area. The procedure also requires an employee background check before granting hosting center access.

In most cases, DTMB was aware that the former employees no longer required access. However, DTMB did not complete the process to remove access.

After bringing this matter to management's attention, DTMB conducted the background checks.

b. Hosting centers had additional physical security control weaknesses. Because of the confidentiality of these weaknesses, we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB management.

RECOMMENDATION

We recommend that DTMB establish adequate physical security in and around the State's hosting centers and switch rooms.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. For the hosting centers, DTMB has already restricted access to only those individuals who require access. DTMB has conducted background checks for all current employees who had not previously received one by the Michigan State Police. In addition, DTMB will implement new monthly reporting and review procedures to strengthen the hosting centers' physical security controls. For the switch rooms, DTMB has already restricted access to only those individuals who require access and will review card key access reports every six months.

FINDING #3

Improvements needed to telecommunication equipment inventory controls.

DTMB did not maintain complete and accurate records of the State's telecommunication equipment and, therefore, could not ensure that all equipment was accounted for and physically protected.

DTMB Technical Standard 1340.00.03 requires the preparation and maintenance of documentation related to the implementation, maintenance, and administration of IT resources, including the resource name and location. Our review of physical inventory controls over telecommunication equipment disclosed:

a. DTMB did not maintain a complete inventory of telecommunication equipment. We noted:

   (1) DTMB utilized two equipment monitoring systems (Orion and Spectrum) and two equipment inventory systems (the Configuration Management Database [CMDB] and the Asset Control System [ACS]). However, none of these systems contained a complete and accurate inventory. We compared the equipment records in Orion with the CMDB data and noted that 268 (8%) of the 3,317 devices in Orion were not included in the CMDB. In addition, 45 (19%) of 232 equipment items in 8 buildings were recorded in one system but not the other. Furthermore, DTMB informed us that it was in the process of adding equipment records into ACS.

   Equipment monitoring and inventory systems should contain complete records to ensure that the information provided by the systems is accurate. In addition, updating multiple systems is inefficient and impairs DTMB's ability to monitor and secure all equipment.

DTMB could not efficiently identify the location of all telecommunication equipment.

   (2) DTMB could not efficiently identify the location of all telecommunication equipment, which could result in inadequate security or delays in locating equipment if repairs are needed. DTMB informed us that equipment location can be recorded in Orion; however, it did not always input the information into Orion.

b. NTSD did not fully implement controls to track all purchased equipment. NTSD tracks new telecommunication equipment using radio-frequency identification (RFID) tags. To monitor the movement of equipment, an RFID reader in the inventory room doorway alerts NTSD employees when equipment leaves the room. However, for equipment purchased between February and April 2015, 8 (9%) of the 93 equipment pieces were not tagged with an RFID tag.

DTMB informed us that these issues were caused by a lack of personnel and financial resources.

RECOMMENDATION

We recommend that DTMB maintain complete and accurate records of the State's telecommunication equipment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB is currently able to identify all major equipment via its equipment monitoring and inventory systems; however, DTMB plans to review its remote out-state located equipment for accuracy. DTMB will continue to make improvements to its inventory processes, which recently included installing and tracking RFID tags to improve and monitor the accuracy of the major equipment inventory in ACS and the CMDB. Additional staffing and funding to improve telecommunication equipment inventory controls will be proposed for management and budgetary approval.

IMPLEMENTING ENVIRONMENTAL CONTROLS

BACKGROUND

Environmental controls* prevent or mitigate damage to facilities and the resources housed within those facilities, reducing the risk of loss of computing services. Environmental controls can minimize and prevent IT service interruptions from fire, smoke, and water leaks. Examples of environmental controls include fire alarms, fire suppression systems, smoke detectors, temperature and humidity controls, voltage control, and emergency lighting.

DCO and NTSD manage environmental controls for the hosting centers, switch rooms, and rooms containing telecommunication equipment.

DTMB has adopted the Building Industry Consulting Service International, Inc., Telecommunications Distribution Methods Manual* (BICSI TDMM) as an industry standard for communication equipment, guidance on equipment installation, physical security, and environmental controls.

AUDIT OBJECTIVE

To assess the adequacy of DTMB's environmental controls in place at locations housing the State's IT resources.

CONCLUSION

Generally adequate.

FACTORS IMPACTING CONCLUSION

- Two of the State's 3 hosting centers were cleaned regularly.
- Two of the 3 hosting centers and 5 of the State's 8 switch rooms had environmental systems in place to monitor mechanical equipment, chilled water supply, and room temperature.
- Material condition related to the lack of environmental controls over IT equipment, primarily in MTRs and TRs.

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

FINDING #4

Adequate environmental controls are not implemented.

DTMB had not implemented adequate environmental controls over IT equipment, which could result in damaged equipment or fire hazards and hinder the work of IT staff at these locations.

We reviewed environmental controls at DTMB's 3 hosting centers, 8 switch rooms, and 163 MTRs and TRs (of which 86 were MTRs), located in 83 of the approximately 790 State office buildings throughout Michigan. We also reviewed environmental controls at DTMB's IT equipment storage warehouse. Our review disclosed:

a. Some switch rooms, MTRs, and TRs that were not reasonably free from dust, food and beverages, and general storage items. We noted:

   (1) Significant dust in 2 (25%) of the 8 switch rooms and 23 (14%) of the 163 MTRs and TRs.

   NTSD and DCO entered into a memorandum of understanding requiring DCO to schedule annual switch room cleanings. However, DCO had not scheduled cleanings in 7 (88%) of the 8 switch rooms for several years. BICSI TDMM states that dust in MTRs and TRs should be minimized. Excessive dust can accelerate wear of mechanical components and clog air filters, causing heat to build up in the equipment.

   (2) Evidence of food or beverages in 5 (63%) of the 8 switch rooms and 20 (12%) of the 163 MTRs and TRs.

   FISCAM recommends that eating and drinking be prohibited in computer facilities. However, DTMB policy did not address eating or drinking in these rooms.

   (3) Storage of general inventory items, such as a propane tank, cleaning supplies, guns, and holiday decorations, in 1 (33%) of the 3 hosting centers, 7 (88%) of the 8 switch rooms, and 122 (75%) of the 163 MTRs and TRs.

   Exhibit 1 presents examples of items we observed. BICSI TDMM states that telecommunication spaces should not be used for general storage, which can hinder the work of IT staff or create a fire hazard. DTMB policy did not address general storage in the hosting centers, MTRs, or TRs.

Telecommunication equipment was susceptible to water damage.

b. Potential water hazards in MTRs and TRs.

BICSI TDMM states that computers and telecommunication equipment should be located away from areas at risk for flooding or raised as high off the floor as possible and should not be located below restrooms and kitchens or near pipes carrying liquids. We identified water damage and risks of future water damage in 3 (38%) of the 8 switch rooms and 39 (24%) of the 163 MTRs and TRs:

(1) Equipment in 1 (13%) of the 8 switch rooms and 10 (6%) of the 163 MTRs and TRs was located next to a hot water heater or water softener or was in a basement without a raised floor.

(2) Two (25%) of the 8 switch rooms and 16 (10%) of the 163 MTRs and TRs were located below restrooms or kitchens and near pipes carrying liquids.

(3) Two (25%) of the 8 switch rooms and 25 (15%) of the 163 MTRs and TRs showed signs of water damage, such as water-stained ceiling tiles.

Facilities lacked fire detection and suppression systems.

c. Inadequate fire detection and suppression systems. We noted:

(1) Eighty-five (52%) of the 163 MTRs and TRs did not have fire alarms. Also, 54 (33%) of the MTRs and TRs did not have a portable fire extinguisher with a current inspection tag. BICSI TDMM states that a fire alarm should be located in the TR and a fire extinguisher should be near the entrance to the room.

(2) Seventy-two (44%) and 71 (44%) of the 163 MTRs and TRs, respectively, did not have smoke detectors or a fire suppression system. Staff at some of the buildings confirmed that the entire building lacked a fire suppression system. BICSI TDMM recommends that smoke detectors and fire suppression systems be installed to minimize fire damage. DTMB Technical Standard 1345.00.02 recommends that fire suppression systems be in place in MTRs, but it does not address fire suppression in TRs. It also does not address the need for fire extinguishers, smoke detectors, or fire alarms.

(3) DTMB's IT equipment storage warehouse did not contain fire suppression or fire detection to protect servers, switches, routers, and computers located in the warehouse. DTMB informed us that it did not

have a policy requiring fire suppression in the warehouse.

Telecommunication equipment was not properly grounded.

d. Ungrounded telecommunication equipment in 51 (31%) of the 163 MTRs and TRs.

   BICSI TDMM recommends that all equipment be properly grounded to decrease the risk of injury or equipment damage from electric shock. DTMB Technical Standard 1345.00.02 requires a telephone grounding bar to be present in MTRs and TRs, but it does not address the need for grounding other equipment in the rooms.

e. Carpeted floors in 24 (15%) of the 163 MTRs and TRs.

   DTMB Technical Standard 1345.00.02 states that carpet should not be used in MTRs and TRs. Carpet increases the risk of static electricity and dust, which could cause a fire or equipment malfunction.

f. No emergency lighting in 77 (90%) of the 86 MTRs.

   DTMB Technical Standard 1345.00.02 requires that MTRs have emergency lighting. Without emergency lighting, DTMB cannot ensure that MTRs can be exited safely during an emergency.

g. Inadequate surge suppression in MTRs.

   Sixteen (19%) of the 86 MTRs were not equipped with transient voltage surge suppressors* (TVSSs) as required by DTMB Technical Standard 1345.00.02. Without TVSSs, DTMB cannot ensure that equipment will be protected in the event of an electrical surge.

The weaknesses existed because DTMB had not established and implemented policies consistent with best practices. Exhibit 2 provides examples of some of the weaknesses identified in this finding.

RECOMMENDATION

We recommend that DTMB implement adequate environmental controls over IT equipment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB has already started cleaning of the out-of-compliance switch rooms and will establish an MTR/TR cleaning schedule. DTMB will ensure

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

that its policies and procedures expressly prohibit eating and drinking in MTRs/TRs, including posting proper signage, consistent with best practices. In addition, DTMB will modify its policies to prohibit use of MTRs/TRs for general storage, consistent with best practices. DTMB will evaluate MTRs/TRs found to have water hazards; however, most MTRs/TRs are located in leased facilities. MTRs/TRs located in leased facilities will be addressed on an individual basis and equipment will be relocated, if reasonable accommodations can be achieved. DTMB will evaluate fire detection and suppression systems, alarms, and emergency lighting to meet BICSI standards. In addition, DTMB will develop a plan to inspect and correct, if necessary, all MTRs/TRs to ensure that equipment has proper grounding and surge suppression.

ESTABLISHING EFFECTIVE GOVERNANCE

BACKGROUND

DCO is responsible for managing and monitoring mechanical equipment, such as air conditioning units, uninterruptible power supplies* (UPSs), and TVSSs, at the hosting centers and switch rooms. This equipment helps ensure that the hosting centers and switch rooms are environmentally controlled by cooling the rooms and providing emergency power and surge protection. Each equipment item has an estimated useful life. DCO tracks the installation dates, schedules regular maintenance, monitors equipment, and makes proposals to DTMB management for replacement.

Control Objectives for Information and Related Technology* (COBIT) is a framework adopted by DTMB as a best practice for IT management and governance.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's governance over physical security and environmental controls at locations housing the State's IT resources.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Maintenance was performed on most mechanical equipment according to the manufacturers' recommended schedule.
- Systems are used to monitor environmental conditions, such as temperature and air quality, and mechanical equipment in 2 of the 3 hosting centers and 5 of the 8 switch rooms.
- As noted in Findings #1 and #4, DTMB had not fully established policies and procedures for physical security and environmental controls.
- Reportable conditions related to mechanical equipment replacement and lack of documentation for TVSS unit maintenance.

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

FINDING #5

Plan is needed for replacement of aging mechanical equipment.

DTMB had not prepared and approved plans for the replacement of mechanical equipment that has exceeded its life expectancy, which could lead to equipment failure and service disruption.

COBIT requires entities to regularly consider the risk of failure and need for replacement of mechanical equipment.

DTMB continued to utilize air conditioning, UPS, and TVSS units that had exceeded the manufacturers' suggested life expectancy at 2 of the 3 hosting centers and 4 of the 8 DTMB-managed switch rooms as follows:

	Hosting Center 1	Hosting Center 2	Switch Rooms
Air Conditioning Units			
Typical life expectancy: 15 years			
Number of units at location	20	9	15
Number of units past life expectancy	0 (0%)	6 (67%)	6 (40%)
Age of units exceeding life expectancy	Not applicable	17 years	20 to 27 years
Uninterruptible Power Supplies (UPSs)			
Typical life expectancy: 15 years			
Number of units at location	10	3	6
Number of units past life expectancy	2 (20%)	0 (0%)	1 (17%)
Age of units exceeding life expectancy	16 years	Not applicable	16 years
Transient Voltage Surge Suppressors (TVSSs)			
Typical life expectancy: 15 years			
Number of units at location	3	4	5
Number of units past life expectancy	2 (67%)	2 (50%)	2 (40%)
Age of units exceeding life expectancy	16 years	18 years	16 years

DCO management informed us that:

- In June 2015, DCO submitted a proposal to upgrade the mechanical equipment at Hosting Center 1, which DTMB management approved and expects to complete within 12 to 18 months.
- Since 2008, DCO submitted 11 proposals to upgrade mechanical equipment in Hosting Center 2. DCO informed us that DTMB management did not approve any of the proposals because they intended to discontinue using the hosting center by 2011.
- DCO did not have a plan to replace mechanical equipment in switch rooms. DCO requested equipment upgrades based on necessity; however, many pieces of mechanical equipment far exceed the typical life expectancy.

Mechanical equipment in the hosting centers and switch rooms are regularly maintained, which reduces the risk of equipment failure but does not eliminate it. Proper planning and authorization to replace mechanical equipment before failure would help ensure that hosting centers and switch rooms continue functioning properly.

RECOMMENDATION

We recommend that DTMB prepare and approve plans for the replacement of mechanical equipment that has exceeded its life expectancy.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB maintains a rigorous hosting center maintenance schedule for all electrical/mechanical infrastructure equipment, which is performed by manufacturer-trained and -certified technicians. All mechanical equipment approaching their end-of-life are evaluated and replaced primarily based on two factors: technician recommendations and budgetary approval. Contingent upon budgetary approval, a contract will be awarded in early 2016 to replace the units that have exceeded their life expectancy, as identified in the audit report.

FINDING #6

Improved documentation is needed to show that preventive maintenance is performed.

DTMB did not maintain documentation to support the completion of required preventive maintenance services for TVSS units. As a result, DTMB could not ensure that TVSS units were properly maintained and functioning at the State's hosting centers and switch rooms.

FISCAM states that hardware maintenance helps prevent unexpected interruptions in network service resulting from hardware equipment failures. FISCAM also states that all maintenance services performed should be documented.

DTMB contracted for preventive maintenance of TVSS units. The contract required the contractor to prepare a summary report of activity performed during preventive maintenance calls.

Our review of preventive maintenance documentation for 2 of the 14 TVSS units in the hosting centers and switch rooms disclosed that DTMB did not obtain the summary report from the contractor. Also, DTMB informed us that the contractor does not provide documentation for maintenance performed on any of the TVSS units. Without documentation, DTMB cannot verify that the maintenance was performed or whether the units need to be replaced.

RECOMMENDATION

We recommend that DTMB maintain documentation to support the completion of required preventive maintenance services for TVSS units.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. Contingent upon budgetary approval, DTMB will replace all TVSS units at Hosting Center 1. As a new site for Hosting Center 2 is expected to be identified by mid-2016, however, these TVSS units will not be replaced. DTMB will review all TVSS units in the switch rooms to schedule maintenance and/or their replacement, as necessary. DTMB will work with vendors to ensure that the proper documentation is maintained to support the preventative maintenance schedules for the TVSS units.

SUPPLEMENTAL INFORMATION

Exhibit #1

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS
OVER INFORMATION TECHNOLOGY RESOURCES
Department of Technology, Management, and Budget

Examples of Items Inappropriately Stored in Hosting Centers, Switch Rooms, MTRs, and TRs
February Through July 2015

Hosting Centers

- Bin full of cables and fixtures
- Shelving units
- Stacks of floor tiles
- Storage totes

Switch Rooms

- Cardboard boxes
- Ceiling tiles
- Filing cabinets
- Ladders
- Mop bucket
- Propane tank
- Printers
- Tables

MTRs and TRs

- Ammunition
- Bicycles
- Christmas trees
- Cleaning/janitorial supplies
- Copy machine
- Filing cabinets/shelving units
- Grill
- Guns
- Holiday decorations
- Icemelt/sidewalk salt
- Ladders
- Large boxes of light bulbs
- Lighter fluid
- Lumber
- Mop bucket
- Office supplies
- Pallets of carpet squares
- Pianos
- Safes
- Shovel
- Tires
- Toilets
- Tools
- Toys for Tots bin
- Tranquilizers (for animals)
- Vacuum cleaners
- Water softener
- Wheelchair

Source: The Office of the Auditor General prepared this exhibit based on observation of hosting centers, switch rooms, MTRs, and TRs.

Exhibit #2

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS
OVER INFORMATION TECHNOLOGY RESOURCES
Department of Technology, Management, and Budget

Examples of Security and Environmental Weaknesses in Switch Rooms, MTRs, and TRs
February Through July 2015

Example of a lack of cleanliness and evidence of food in a TR.

Photograph provided by DTMB.

This exhibit continued on next page.

Open and unlocked door, general storage, and unsecured cabling in a TR.

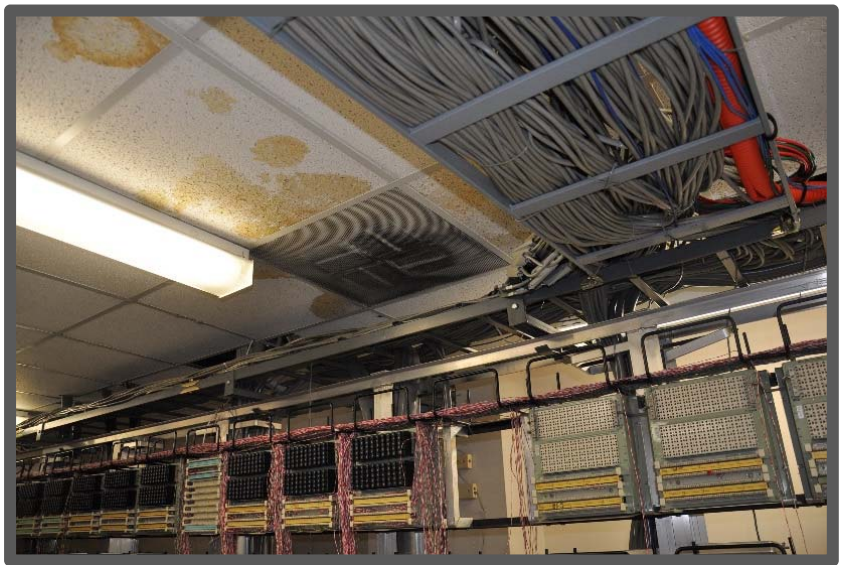
Photograph taken by Office of the Auditor General staff.

This exhibit continued on next page.

TR used for storage (boxes and holiday decorations).

TR with doors that do not lock.

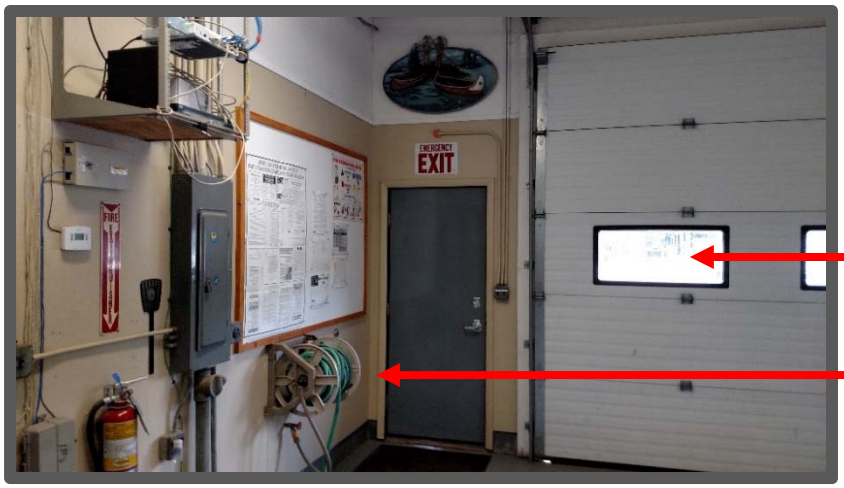
TR with general storage (guns, safes, and ammunition).



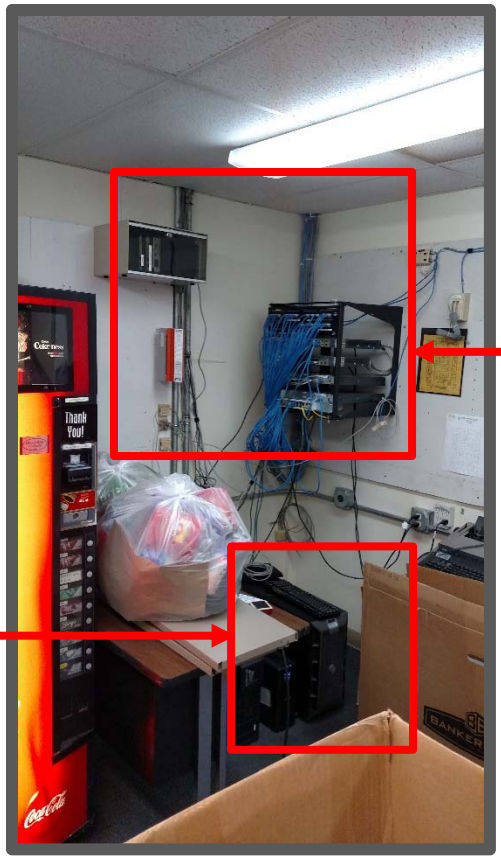
Water-damaged ceiling in a switch room above telecommunication equipment.

Photographs taken by Office of the Auditor General staff.

This exhibit continued on next page.



Telecommunication equipment located in a garage rather than a designated TR. Garage doors do not have safety glass. Garden hose near equipment.



Telecommunication equipment located in a break room rather than in a designated TR. Servers are on the floor. Break room has carpeted flooring; general storage (boxes, trash, and typewriter); and food and beverages (vending machine) near the equipment.

Photographs taken by Office of the Auditor General staff.

DESCRIPTION

The State's IT resources are located in numerous computer facilities around the State. These facilities include three computer hosting centers, eight switch rooms, numerous TRs, and an IT equipment storage room. IT resources located in these facilities include computer servers, mainframe computers, storage devices, telecommunication equipment, network equipment and wiring, and backup power devices.

Hosting Centers

DCO manages the three hosting centers where the majority of the State's servers are located. The hosting centers also contain mechanical equipment, such as backup generators, air conditioning units, and UPSs, which help to ensure that servers operate properly on a daily basis and in emergency situations.

Switch Rooms

Switch rooms connect MTRs from multiple buildings and route network traffic to the hosting centers to access the appropriate servers to store or retrieve data. There are eight DTMB-managed switch rooms throughout the State.

DCO and NTSD share responsibility for the switch rooms with a memorandum of understanding documenting each division's responsibilities. DCO is responsible for ensuring physical security, scheduling annual room cleanings, and maintaining mechanical equipment. NTSD approves these activities; provides the necessary funding; and maintains the switches, routers, and other telecommunication equipment.

Telecommunication Rooms (TRs)

Each of the approximately 790 State office buildings located throughout Michigan include at least one TR containing equipment that provides the network, Internet, and telephone connections from individual computer work stations within the building to the State's IT network. Large or multi-level buildings generally have multiple TRs with at least one TR per floor. The TRs connect to the buildings' MTR, which connects to one of the State's switch rooms.

NTSD performs the initial setup and monitoring of telecommunication equipment in MTRs and TRs. The initial setup includes installing telephone and network equipment and connecting that equipment to individual computer work stations. After installation, the office or building manager is responsible for physical security of MTRs and TRs.

Equipment Storage Warehouse

DTMB's IT equipment storage warehouse contains new equipment awaiting delivery to the hosting centers, switch rooms, and TRs. The warehouse also contains retired equipment awaiting disposal.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the physical security and environmental controls over locations housing DTMB-managed IT resources. 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 did not include IT resources managed by other State agencies.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2012 through July 31, 2015.

METHODOLOGY

We conducted a preliminary survey of DTMB's physical security and environmental controls to formulate a basis for defining our audit objectives and scope. During our preliminary survey, we:

- Interviewed DTMB management and staff to obtain an understanding of controls and procedures.
- Reviewed applicable DTMB policies and procedures.
- Reviewed industry best practices.
- Toured 2 of the State's 3 hosting centers and selected switch rooms and TRs to gain an understanding of physical security and environmental controls in place.

OBJECTIVE #1

To assess the adequacy of DTMB's physical security controls in place at locations housing the State's IT resources.

To accomplish this objective, we:

- Compared DTMB's physical security control policies with industry best practices.
- Toured the hosting centers, switch rooms, and the IT equipment storage warehouse to evaluate physical security controls.

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

- Judgmentally selected 83 of the approximately 790 State office buildings located throughout the State to tour and evaluate physical security controls over the TRs.

- Judgmentally selected and evaluated the access rights of individuals with hosting center, switch room, and TR access for appropriateness with job roles and responsibilities.

- Reviewed after-hours perimeter security for two hosting centers.

OBJECTIVE #2

To assess the adequacy of DTMB's environmental controls in place at locations housing the State's IT resources.

To accomplish this objective, we:

- Compared DTMB's environmental control policies to industry best practices.

- Reviewed agreements between DCO and NTSD related to the switch rooms.

- Toured the hosting centers, switch rooms, and the IT equipment storage warehouse to evaluate environmental controls.

- Reviewed the contract for cleaning the hosting centers and switch rooms and assessed whether cleanings were performed in accordance with contract requirements.

- Judgmentally selected 83 of the approximately 790 State office buildings located throughout the State to tour and evaluate environmental controls over the TRs.

- Performed a reconciliation of the telecommunication equipment recorded in DTMB's monitoring systems to determine whether all equipment was accounted for and monitored.

OBJECTIVE #3

To assess the effectiveness of DTMB's governance over physical security and environmental controls at locations housing the State's IT resources.

To accomplish this objective, we:

- Compared the age of mechanical equipment (such as air conditioning units, UPSs, and backup batteries) at the hosting centers and switch rooms to the manufacturers' recommended useful life.

- Assessed DTMB's strategic plans for the hosting centers, including long-term viability and planning for future capacity needs.

- Reviewed the hosting center and switch room equipment maintenance contract.

- Judgmentally selected hosting center and switch room equipment to evaluate whether routine maintenance was performed and supporting documentation was maintained.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions and 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 audits on an exception basis.

AGENCY RESPONSES

Our audit report contains 6 findings and 6 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all 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 audit 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 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

ACS	Asset Control System.
adequate	As much or as good as necessary for some requirement or purpose.
Building Industry Consulting Service International, Inc., Telecommunications Distribution Methods Manual (BICSI TDMM)	Reference manual published by Building Industry Consulting Services International, Inc. (BICSI), which describes current industry best practices for the information technology industry.
CMDB	Configuration Management Database.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and guidelines published by the IT Governance Institute as a generally applicable and acceptable standard for good practices for controls over information technology.
DCO	Data Center Operations.
DTMB	Department of Technology, Management, and Budget.
environmental control	A control that prevents or mitigates damage to facilities and interruptions in service through early detection of problems such as fire, smoke, and water leaks.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards.*
hosting center	A building or a portion of a building whose primary function is to house a computer room and its support systems.
information technology (IT)	Anything related to computing technology, such as networking, hardware, software, the Internet, or the people who work with these technologies.

main telecommunication room (MTR)	A TR that provides the pathway for data coming into and out of a building. MTRs connect all of the TRs in a building to the switch rooms.
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.
NTSD	Network and Telecommunications 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.
physical security control	A control that restricts physical access to computer resources and protects them from intentional or unintentional loss or impairment.
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.
RFID	radio-frequency identification.
switch room	A room that connects MTRs from multiple buildings and routes network traffic to the hosting centers to access the appropriate servers to store or retrieve data.
telecommunication room (TR)	An enclosed architectural space for equipment that provides data and telephone connections. There is typically one TR per floor that connects to the MTR within the building.

transient voltage surge suppressor (TVSS)	Mechanical equipment that protects data processing and other critical equipment from lightening and other sources by suppressing short blasts of energy (transient surges) on electrical circuits.
uninterruptible power supply (UPS)	Mechanical equipment that provides nearly instantaneous power when the main utility power source fails, allowing either time for power to return or for the user to shut down the system or equipment normally by closing running computer system applications and using the operating system to shut down the system.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


OAG
Office of the Auditor General
Independent
Objective
Transparent