Office of the Auditor General
Performance Audit Report

IT Equipment Surplus and Salvage

Department of Technology, Management, and Budget

January 2020

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

071-0515-19

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.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

IT Equipment Surplus and Salvage

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0515-19

Released:
January 2020

IT equipment is regularly purchased and used by State of Michigan employees to process and store data for State government operations. As this equipment becomes surplus, obsolete, or out of warranty, the State must dispose of these items in a safe and secure manner. To accomplish this, DTMB has contracted with a third-party vendor for the sanitization and disposal of unneeded IT equipment, including desktop computers, laptop computers, servers, storage and networking devices, smart phones, and tablet computers. State employees use the Automated Asset Recovery Program (AARP) System to submit unneeded equipment to DTMB for surplus and salvage. DTMB Delivery, Warehouse, and Surplus Services primarily handles the transfer and storage of equipment until vendor pickup. Workstations that are fit for reuse are stored as agency stock.

Audit Objective	Conclusion
Objective #1: To assess the sufficiency of DTMB's efforts to prevent the unauthorized disclosure of data on surplus and salvage IT equipment.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB, in conjunction with the vendor, did not have certification of proper disposal for 25 (16%) of 154 equipment items sampled and did not track sufficient details for the disposal of smart phones and certain tablet computers (Finding #1).	X		Agrees
The IT equipment that DTMB verified had been sanitized was known to the vendor prior to applying the sanitization process. Selecting the equipment after sanitization would provide DTMB with better assurances that all equipment was properly sanitized. Also, DTMB did not select all types of computer equipment for verification (Finding #2).		X	Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
The third-party audit of DTMB's IT equipment sanitization and disposal vendor did not include review of the vendor's data privacy and information security program (Finding #3).		X	Agrees
DTMB did not verify that its vendors effectively sanitized leased multi-function printers prior to disposal. Those printers may house images of any scanned, copied, or faxed documents within their local memory (Finding #4).		X	Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DTMB's efforts to prevent and detect the theft of surplus and salvage IT equipment.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not restrict access to surplus and salvage IT equipment to only employees who required access. Forty-nine percent of employees reviewed did not require access to the designated surplus and salvage area. Also, DTMB did not securely store untracked smart phones and hard drives within the designated storage area. The audit team's removal from the building of 6 smart phones awaiting disposal went undetected (Finding #5).	X		Agrees
DTMB did not ensure proper payments from the sanitization vendor by reconciling with the surplus and salvage IT equipment sent for disposal. We identified 222 pieces of IT equipment provided to the vendor for sanitization in July 2018 that were unaccounted for in asset settlement reports tied to payments (Finding #6).		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

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

January 29, 2020

Ms. Tricia L. Foster, Director
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Foster:

This is our performance audit report on IT Equipment Surplus and Salvage, 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 to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, 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

IT EQUIPMENT SURPLUS AND SALVAGE

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

PREVENTION OF UNAUTHORIZED DISCLOSURE OF DATA ON SURPLUS AND SALVAGE IT EQUIPMENT

BACKGROUND

Sanitization* is the process of rendering access to data on media* infeasible and is a key element in ensuring data confidentiality*. Loss of confidentiality is the unauthorized disclosure of information. Organizations should sanitize or destroy IT equipment before its disposal* or release for reuse outside of the organization to prevent unauthorized individuals from gaining access to and using the information contained on the media.

The Department of Technology, Management, and Budget (DTMB) contracts with a third-party vendor for the sanitization and disposal of IT equipment. DTMB receives these services at no charge in exchange for allowing the vendor to resell IT equipment that still has residual value after it has been sanitized. If equipment does not have residual value, the vendor will recycle the equipment in a way that sanitizes all State data on that piece of equipment.

State agencies initiate the disposal process by submitting a request through DTMB's Automated Asset Recovery Program* (AARP) System. The equipment will be either put into agency stock for reuse or disposed of and, when necessary, removed from the official inventory record. DTMB maintains two central IT equipment inventories: the Information Technology Asset Management System (ITAM) for desktop computers, laptop computers, and Windows tablets and the Configuration Management Database* (CMDB) for servers, stand-alone storage devices, and network equipment.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to prevent the unauthorized disclosure of data on surplus and salvage IT equipment.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- State-owned IT equipment that we selected from the third-party vendor's inventory was effectively sanitized.
- DTMB implemented some standards and procedures related to surplus and salvage IT equipment.
- The ITAM and CMDB inventories were substantially accurate regarding asset lifecycle status in relation to whether the State still maintained possession of the asset.

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

- One material condition* related to insufficient controls to ensure that DTMB properly sanitized and disposed of all surplus and salvage IT equipment (Finding #1).

- Three reportable conditions* related to an improved process for verifying the vendor's sanitization efforts, the need for an independent third-party audit of the vendor's data privacy and information security* program, and insufficient controls to verify that leased printers were effectively sanitized prior to disposal (Findings #2 through #4).

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

FINDING #1

Controls needed to ensure sanitization and disposal.

DTMB did not fully establish controls to ensure that its vendor properly sanitized and disposed of all surplus and salvage IT equipment. Media sanitization is a key element in ensuring confidentiality and preventing the unauthorized disclosure of data stored on surplus and salvage IT equipment.

The National Institute of Standards and Technology* (NIST) states that organizations should sanitize digital media using approved methods and that the sanitization should be tracked, documented, and verified. NIST also states that, following sanitization, a certificate of media disposition should be completed for each piece of media that has been sanitized.

DTMB uses the AARP System to process agency disposal requests for IT equipment owned by the State. Disposal requests include IT equipment tracked by serial number, such as desktop computers, laptop computers, servers, stand-alone storage devices, and network equipment. In addition, agencies may dispose of non-centrally inventoried devices, such as smart phones, non-Windows tablets, hard drives, and other miscellaneous devices.

DTMB assigns a pallet number to track IT equipment identified for disposal within the AARP System and places the equipment on that pallet for vendor pickup. Pallets containing desktop computers, laptop computers, and servers are added to a manifest which DTMB provides to the vendor so that equipment can be scanned for tracking during pickup. Our review disclosed:

a. DTMB did not have procedures to:

   (1) Monitor disposal records for stand-alone storage devices and network equipment for which the pallet number was left blank.

   DTMB has a procedure to monitor blank pallet numbers on disposal records for appropriateness; however, it applies to only desktop computers, laptop computers, and servers. Although blank pallet numbers may be appropriate in certain situations, such as warranty replacements that were not sent out for disposal, they could also indicate that IT equipment was not sent to the vendor for proper sanitization and disposal.

   (2) Review all devices that were assigned to a pallet number and ensure that the devices were included on the appropriate manifest for pickup.

   Devices assigned a pallet number, but not added to a manifest, could indicate that the device did not arrive at the vendor's facility and was not properly disposed of.

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

(3) Use a manifest to track network equipment sent to the vendor.

Network equipment includes switches, routers, and firewalls. Adding these devices to a manifest would help ensure that sufficient chain of custody documentation exists and that all network equipment assigned to a pallet is accounted for by the vendor during pickup.

b. DTMB did not establish procedures to reconcile vendor disposal certificates with its equipment disposal records. Disposal certificates are the vendor's assertion that surplus and salvage equipment has been properly disposed of. Our review disclosed that DTMB did not have disposal certificates for:

(1) 15 (22%) of 68 sampled AARP disposal requests.

DTMB and the vendor could not locate disposal certificates for 25 (16%) of 154 disposal records reviewed.

DTMB followed up with the vendor, who was able to locate 6 of the missing certificates leaving 9 (13%) of 68 devices without a disposal certificate.

(2) 5 (12%) of 43 sampled ITAM records for retired desktop computers, laptop computers, and Windows tablets.

DTMB followed up with the vendor, who was able to locate 4 of the missing certificates leaving 1 (2%) of 43 devices without a disposal certificate.

(3) 24 (56%) of 43 sampled CMDB records for retired servers, stand-alone storage devices, and network equipment.

DTMB followed up with the vendor, who was able to locate 9 of the missing certificates leaving 15 (35%) of the 43 devices without a disposal certificate.

Reconciliation controls for disposal certificates would help ensure that the vendor properly sanitized and disposed of all IT equipment received from the State.

c. DTMB did not track smart phones, non-Windows tablets, and individual hard drives at a detailed level in the AARP System. AARP submitters may add smart phones, non-Windows tablets, and hard drives to the online AARP disposal request form. However, information such as serial number, device type, model, and asset tag were not tracked. DTMB informed us that the sanitization vendor still treats these items as secure devices that must be sanitized and tracked; however, without including sufficient details in the disposal request, DTMB is unable to maintain chain of custody documentation that allows it to validate

DTMB did not track smart phones, non-Windows tablets, and hard drives through the disposal process using the AARP System.

when a device was received for disposal, provided to the vendor, and properly sanitized.

DTMB informed us that these issues were primarily the result of the complexity that arises from the number of DTMB divisions involved in the inventory tracking and disposal process and because devices such as smart phones are owned and inventoried by all State departments, causing the central management of full lifecycle controls to be difficult to implement.

We consider this finding to be a material condition because of the amount of confidential and sensitive data maintained and used by the State. These controls are a critical aspect of ensuring that data is protected when the State disposes of IT equipment.

RECOMMENDATION

We recommend that DTMB fully establish controls to ensure that its vendor properly sanitizes and disposes of all surplus and salvage IT equipment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

DTMB agrees with the recommendation to fully establish procedures. DTMB updated internal procedures to include tracking network equipment and standalone storage devices (December 2019). In addition, DTMB developed internal procedures to validate the existence of disposal or sanitization certificates (December 2019). Furthermore, DTMB developed an internal procedure to ensure that all devices assigned to a pallet are also assigned to a shipping manifest (January 2020).

DTMB agrees with the OAG's recommendation to track smart devices and individual hard drives as IT assets at a detailed level through the disposal process to maintain chain of custody documentation. DTMB will implement controls to increase the chain of custody documentation for these devices as part of the disposal process (August 2020). DTMB utilizes additional controls to reduce the risk of unauthorized disclosure of State data. These controls include:

- *DTMB utilizes an automated system to administer data security for State of Michigan (SOM) owned and managed smart devices.*
    - *Only devices enrolled and compliant with the system's security policies can access State data. Devices must be approved prior to enrollment.*
    - *A unique passcode is required to access State data on smart devices.*

- *State data cannot be accessed via a smart device if the device does not communicate with the State's system for a specified number of days.*

- *State data on a smart device is automatically wiped after a specified number of unsuccessful passcode attempts or when reported as lost or stolen.*

- *DTMB will ensure that hard drives for SOM-owned and managed computers are encrypted in accordance with Technical Standard 1340.00.170.03.*

- *DTMB sanitizes physical server hard drives to Department of Defense specifications as a part of the decommission process.*

- *As of November 2019, DTMB ensured that smart devices and individual hard drives are secured in locked bins once the devices are received at the State's IT-Depot. DTMB maintains a chain of custody for the bins during the transfer to the vendor.*

- *Smart devices are sanitized by the vendor when the devices can be logically accessed. The vendor shreds all individual hard drives and those smart devices which could not be sanitized.*

DTMB delegated the purchase and issuance of smart devices to State agencies. State agencies are responsible for ensuring that State data is removed from storage media prior to disposal in accordance with Technical Standard 1340.00.110.04. DTMB will continue to work with agencies in clarifying the roles and responsibilities for sanitizing various media when using the AARP system.

FINDING #2

Improvements needed over vendor sanitization verification.

DTMB should improve its process for verifying the effectiveness of its media sanitization vendor's efforts. Proper sanitization helps ensure that any confidential or sensitive information stored on IT equipment is fully deleted prior to disposal by the vendor.

The sanitization contract requires that, prior to the resale or recycling of IT equipment, the vendor must sanitize or destroy each hard drive or device capable of storing data. According to NIST, verifying the sanitization of data is an essential step to maintaining confidentiality and can be accomplished through representative sampling applied to a selected subset of media.

DTMB uses a quarterly audit process in which it selects 10 hard drives from a mix of desktop and laptop computers to assess the effectiveness of the sanitization performed by the vendor. Our review disclosed:

a. DTMB selected the 10 hard drives prior to the vendor sanitization process. After DTMB's selection of the drives, the vendor sanitized them and provided them back to DTMB for audit. Although this sequence allowed DTMB to verify the effectiveness of the sanitization procedures applied, revising the quarterly audit process to select equipment after the vendor has performed its sanitization would better enable DTMB to ensure that the vendor is applying effective sanitization procedures and removing data from all equipment.

b. DTMB selected only hard drives from desktop and laptop computers for audit, even though the vendor is responsible for sanitizing other types of equipment, such as network devices, printers, servers, smart phones, and tablets. The tools and processes used to sanitize IT equipment can vary depending on the type of device. The vendor has the option to resell the equipment if the vendor determines that the equipment has resale value.

   The State's IT equipment awaiting resale by the vendor as of August 8, 2019 included 63 iPhones, 150 desktop computers, and 20 laptop computers. At different points in time, the inventory awaiting resale may contain additional types of computer equipment sent for disposal. Because DTMB's audit procedure is to select only hard drives from desktop and laptop computers, DTMB does not obtain assurance that these other types of equipment have been effectively sanitized by the vendor.

DTMB informed us that it selected IT equipment prior to sanitization by the vendor because waiting until after it was sanitized would make the process more complex. DTMB also informed us that its audit efforts focused only on hard drives from desktop and laptop computers because they made up a large percentage of the IT equipment sanitized by the vendor.

RECOMMENDATION

We recommend that DTMB improve its process for verifying the effectiveness of its media sanitization vendor's efforts.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and has complied.

DTMB updated its internal procedure to verify the vendor sanitization process (October 2019). DTMB now selects devices for verification after vendor sanitization has occurred and the equipment is available for resale. In addition to hard drives, DTMB now includes other potentially data bearing assets in the verification sample. DTMB implemented the updated procedure (November 2019).

FINDING #3

Independent audit of data privacy and information security should be obtained.

DTMB did not ensure that its IT equipment sanitization and disposal vendor obtained a third-party audit of its data privacy and information security program. An annual third-party audit would help ensure the security and confidentiality of any State data on IT equipment that was sanitized or disposed of by the vendor.

The contract requires that, no less than annually, the vendor must conduct a comprehensive independent third-party audit of its data privacy and information security program and provide audit findings to the State. According to NIST, when outsourcing the sanitization and destruction of IT equipment, an organization must exercise due diligence, which could include reviewing an independent audit of the disposal company's operations.

The vendor obtained an annual third-party audit to assess compliance with ISO 14001:2015, which is a standard published by the International Organization for Standardization that specifies the requirements for an environmental management system and can be used to enhance environmental performance. However, it did not cover the vendor's data privacy and information security controls, including a review of physical, technical, administrative, and organizational safeguards that ensure the security and confidentiality of State data. Also, it did not include testing designed to assess the effectiveness of controls implemented to protect against threats* and the unauthorized disclosure, access to, or use of State data on surplus and salvage IT equipment.

DTMB performs its own security checklist audit every two years; however, the most recent checklist audit did not include tests designed to assess the operating effectiveness of controls or a detailed breakdown of vendor policies and procedures to ensure compliance with State IT policies and standards.

DTMB informed us that it was not aware that the third-party audit was not a comprehensive review of the vendor's data privacy and information security program and has begun working with the vendor to address the issue.

RECOMMENDATION

We recommend that DTMB ensure that its IT equipment sanitization and disposal vendor obtains a third-party audit of its data privacy and information security program.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and has complied.

DTMB updated its internal procedure to ensure that the vendor is audited annually by an independent third party for compliance with the vendor's data privacy and information security program. DTMB also requires the vendor to provide the audit report to the State (November 2019).

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

An independent third party audited the vendor's data privacy and security program and provided the report to DTMB (November 15, 2019).

FINDING #4

Verification of leased printer sanitization effectiveness needed.

DTMB did not fully establish controls to verify that leased multi-function printers were effectively sanitized prior to disposal. Effective sanitization techniques are critical to the process of ensuring that sensitive data is protected from unauthorized disclosure.

NIST states that verifying the sanitization of data is an essential step to maintaining confidentiality and can be accomplished through representative sampling applied to a selected subset of media.

The State leases multi-function printers, which are used for printing, scanning, copying, and faxing, from three different vendors. Multi-function printers have local memory that can store recent documents. DTMB uses servers to manage print queues and remove the risk of printed files being stored locally; however, any scanned, copied, or faxed documents may still be saved on the printer's local memory. Stored documents could include confidential or sensitive information, such as tax returns, health data, or other information used in the day-to-day activities performed using the printer. Each vendor has implemented security features that encrypt a multi-function printer's hard drive using an encryption key specific to that printer. This prevents another device from decrypting that data if the hard drive was removed. At the end of a lease, printers are returned to the vendor who is responsible for the sanitization of local memory on the printers.

DTMB verifies that the vendor completed a certification form asserting that it sanitized the printers. However, DTMB does not perform any procedures to verify that the sanitization occurred or to assess that the tools used effectively removed all data. Although certification is an important part of the disposal process, NIST states that verifying sanitization is a critical aspect of protecting any confidential or sensitive data that may be stored on the devices.

DTMB informed us that it believed that its sanitization process was sufficient to ensure that all devices had been sanitized and that risk had been reduced via compensating controls, such as encryption security features.

RECOMMENDATION

We recommend that DTMB fully establish controls to verify that leased multi-function printers are effectively sanitized prior to disposal.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and utilizes controls to reduce the risk of unauthorized disclosure of State data including:

- *Each vendor implements security features that encrypt a multi-function printer's hard drive using an encryption key*

specific to that printer. This prevents another device from decrypting that data if the hard drive was removed.

- *All documents stored on multifunction devices are encrypted.*
- *Any stored documents are wiped from devices after a maximum specified number of hours.*
- *Vendors complete and provide forms certifying the vendor has sanitized each device. DTMB utilizes a process to verify a certificate is provided for each device upon decommission.*
- *Prior to a device family being made available for lease, Michigan Cyber Security (MCS) security approval is obtained.*

DTMB will assess the options available for process changes to ensure that the vendors' sanitization efforts are working as intended (August 2020), coordinating with DTMB, State agencies, and vendors, to assure that the risks and costs are identified.

PREVENTION AND DETECTION OF THEFT OF SURPLUS AND SALVAGE IT EQUIPMENT

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 and information located within the facility.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. For access controls to be effective, they should be properly authorized, implemented, and maintained.

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's efforts to prevent and detect the theft of surplus and salvage IT equipment.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Our review of surveillance video from the designated surplus and salvage area showed no signs of suspicious activity.
- Reports of lost and stolen IT equipment indicated that equipment generally was not lost or stolen during the disposal process.
- DTMB implemented some standards and procedures to prevent and detect the theft of surplus and salvage IT equipment.
- One material condition related to the need to fully implement physical security controls protecting surplus and salvage IT equipment (Finding #5).
- One reportable condition related to establishing reconciliation controls for payments received from the vendor for surplus and salvage IT equipment (Finding #6).

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

FINDING #5

Improved physical security controls needed.

DTMB did not fully implement physical security controls over the State's surplus and salvage IT equipment, which could lead to unauthorized employees gaining access to IT equipment, undetected theft of equipment, or unauthorized disclosure of sensitive or confidential information.

SOM Technical Standard 1320.00.110.01 requires media to be protected until destroyed or sanitized. SOM Technical Standard 1320.00.120.01 requires physical access to be authorized based on role and a restricted area to be used to control access to sensitive information, such as personally identifiable information (PII).

DTMB gathers surplus and salvage IT equipment from State agencies and stores the equipment in an open designated area within a warehouse building. Employees must be granted approval to access the building. As of June 2019, 357 employees had access to the building. Our review disclosed:

a. DTMB did not restrict access to the surplus and salvage area beyond general building access. We sampled 43 of 357 employees with building access to review for the principle of least privilege* and proper granting of approvals by DTMB. We noted:

49% of employees reviewed did not require access to the State's surplus and salvage IT equipment area for their job responsibilities.

(1) 21 (49%) of 43 employees did not require access to the State's surplus and salvage IT equipment area for their job responsibilities. The 21 employees' job responsibilities necessitated that they have access to the building; however, because of how access to the building is configured, the employees were also granted access to the surplus and salvage area, which does not meet the principle of least privilege.

(2) 5 (12%) of 43 employees did not have approval for at least one access right. Access to the building is granted via access rights to various card readers. These card readers determine which doors within the building an employee can gain entry through. As a result, 5 of 43 employees had unauthorized access to various building doors.

(3) 3 (7%) of 43 employees had access to the building during time frames that exceeded their documented approved access.

b. DTMB did not securely store untracked devices, such as smart phones, non-Windows tablets, and hard drives, within the designated surplus and salvage storage area. Not securing these devices increases the risk that they could be taken from the building undetected and potentially expose State data to unauthorized disclosure.

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

Additional security, such as storing the devices in locked bins or cabinets, would help prevent the theft of these devices and unauthorized disclosure of PII. We performed the following audit procedures:

- Removed smart phones stored in open boxes within the surplus and salvage area from the building without DTMB's detection on 4 of 4 attempts. For 3 of the attempts, an auditor who was not assigned to this audit entered the building to attempt to remove smart phones during normal work hours while DTMB employees were in the general area. For 1 of the attempts, an auditor who was assigned to this audit stayed after normal work hours to remove a smart phone from the building. In total, the auditors' removal of 6 smart phones from the building went undetected. (The auditors had been granted visitor access or standard access as part of their audit responsibilities to emulate employees who would already have access to the building. Agency management was made aware of our audit procedures prior to execution.)

We removed 6 smart phones awaiting sanitization and disposal from the designated storage area without DTMB's detection.

- Reviewed the contents of 21 hard drives stored in an open bin within the designated surplus and salvage area for confidential or sensitive data. We found confidential or sensitive data on 6 (29%) of the 21 hard drives. DTMB began storing hard drives in locked bins in July 2019 during our audit.

DTMB informed us that, because the building has security cameras and is secured to allow only authorized State employees access, additional access restrictions were not deemed necessary for the designated surplus and salvage IT equipment area.

We consider this finding to be a material condition because of the number of employees with access to the surplus and salvage IT equipment who do not require it for their job responsibilities and the presence of untracked IT equipment, such as smart phones, for which it is difficult to detect if theft has occurred.

RECOMMENDATION

We recommend that DTMB fully implement physical security controls over the State's surplus and salvage IT equipment.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

DTMB agrees with the need to ensure access rights to the building are appropriate. DTMB is establishing an internal procedure to review access rights to the building, including

appropriate time frames (January 2020). Additionally, DTMB utilizes existing processes to remove building access rights when appropriate.

DTMB also agrees with the recommendation to securely store untracked devices to reduce the risk of unauthorized access to State data. DTMB began storing smart devices (phones and non-window tablets) in locked bins as of November 2019. As noted in the finding, DTMB began storing hard drives and loose media in locked bins in July 2019.

DTMB agrees that it has not fully restricted access to the surplus and salvage area beyond general building access. Implementing further physical access restrictions to the area would require considerable changes to the existing building, impact Depot operations as well as other operations within the building, and require additional funds. DTMB will consider the OAG's recommendation when additional funding becomes available.

DTMB utilizes existing controls to reduce the risk of unauthorized access to State of Michigan data, such as:

- *DTMB now secures smart devices and loose media in locked bins (November 2019) reducing the risk that unauthorized individuals are able to remove this equipment from the area.*
- *Visitors are escorted within the building.*
- *DTMB is establishing an internal procedure to review access rights to the building, including appropriate time frames (January 2020).*
- *DTMB has security cameras at entry points and throughout the surplus and salvage IT equipment area. DTMB Central Control monitors the video which may be utilized for forensic analysis.*
- *The building dock area is gated with a security guard on duty to restrict unauthorized access.*

FINDING #6

Controls needed to reconcile vendor payments.

DTMB did not establish controls to reconcile payments received from its media sanitization vendor with surplus and salvage IT equipment sent for disposal. Reconciliations would help ensure that DTMB was paid for all qualifying IT equipment sent to the vendor for sanitization and disposal. In fiscal year 2019, DTMB received $346,514 from the vendor for surplus and salvage IT equipment.

The contract requires the vendor to pay DTMB set rates for certain types of IT equipment that meet cosmetic conditions and function sufficiently for the equipment to have resale value. DTMB will not receive payment for equipment that has significant cosmetic damage, is missing key components, or is obsolete.

Payments from the vendor to DTMB should reconcile with monthly vendor credit memorandums that summarize the amount paid and with asset settlement reports, which track IT equipment by serial number and identify the condition of the equipment and the amount to be paid. DTMB did not reconcile payments received with the asset settlement reports or the asset settlement reports with the manifest records of surplus and salvage IT equipment sent to the vendor.

We reconciled IT equipment and payments for July 2018. DTMB scheduled three IT equipment pickups with the vendor and generated manifests that documented, by serial number, the IT equipment to be picked up. We compared the IT equipment from the three manifests with the vendor asset settlement reports provided to DTMB from July 2018 through July 2019 and identified 222 (9%) of 2,452 serial numbers on the manifests that were not accounted for in a settlement report as follows:

Equipment Type	Missing Serial Numbers
Desktop computers	167
Servers	31
Laptop computers	20
Other	2
Windows tablets	1
Network equipment	1
Total	222

Because these serial numbers were not included on an asset settlement report, DTMB could not determine if the equipment failed the cosmetic and functionality tests or if DTMB should have received payment for these items.

DTMB informed us that, because of the number of DTMB divisions involved in the disposal process, it was unclear who was responsible for performing reconciliations and that the divisions were unaware that reconciliations were not being performed.

Development of a written procedure would help establish the roles and responsibilities for payment reconciliation controls.

RECOMMENDATION

We recommend that DTMB establish controls to reconcile payments received from its media sanitization vendor with surplus and salvage IT equipment sent for disposal.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and has complied. DTMB developed and implemented an internal procedure to reconcile payments received from its sanitization vendor to IT equipment sent for disposal (November 2019).

PROCESS DESCRIPTION

IT equipment is regularly purchased and used by State of Michigan employees to process and store data for State government operations. As this equipment becomes surplus, obsolete, or out of warranty, the State must dispose of these items in a safe and secure manner. DTMB contracted with a third-party vendor for the sanitization or disposal of surplus IT equipment, including desktop computers, laptop computers, servers, storage and networking devices, smart phones, and tablet computers.

The State's primary method for disposing of equipment is the AARP System. State employees use this system to notify DTMB of unneeded IT equipment, which is then evaluated to determine if it is fit for reuse or should be disposed of via a vendor. Retired equipment is removed from DTMB's official inventory of record. Workstations that are fit for reuse are stored at the DTMB Depot* as agency stock. DTMB Delivery, Warehouse, and Surplus Services primarily handles the transfer and storage of equipment until it is picked up by the vendor at the Depot location.

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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the processes and records related to the surplus and salvage of IT equipment. 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered July 1, 2015 through September 30, 2019.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of DTMB's IT equipment surplus and salvage operations to formulate a basis for establishing our audit objectives and defining our audit scope and methodology. During our preliminary survey, we:

- Interviewed DTMB management and staff regarding their functions and responsibilities.
- Reviewed the contract between DTMB and the third-party vendor responsible for IT equipment sanitization and disposal.
- Interviewed the third-party vendor regarding its processes and responsibilities for sanitizing the State's IT equipment.
- Reviewed applicable DTMB policies, standards, and procedures.
- Analyzed data for payments received from the third-party vendor for surplus and salvage IT equipment.

OBJECTIVE #1

To assess the sufficiency of DTMB's efforts to prevent the unauthorized disclosure of data on surplus and salvage IT equipment.

To accomplish this objective, we:

- Assessed the effectiveness of the third-party vendor's sanitization for a selection of 20 pieces of State IT equipment held by the vendor for resale.

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

- Reviewed the State's surplus auction Web site from June 25, 2019 through September 6, 2019 to confirm that State-owned IT equipment was not being improperly sold through this Web site.

- Evaluated the independent third-party audit of the sanitization vendor to assess whether the vendor's data privacy and information security program was sufficiently covered by the audit.

- Assessed DTMB's process for validating that the State's IT equipment was effectively sanitized by the third-party vendor.

- Tested the accuracy of lifecycle status for randomly sampled ITAM and CMDB inventory records to verify that equipment listed as active or not salvaged had not been improperly disposed of outside the established disposal process as follows:

    - 43 of 9,419 records from ITAM.

    - 43 of 7,476 records from CMDB.

- Compared the information captured in vendor certificates of disposal and other reports provided to the State with best practice recommendations.

- Interviewed 20 executive branch agencies to gain an understanding of the guidance that DTMB provided in regard to the disposal of IT equipment that was not centrally inventoried by DTMB.

- Randomly and judgmentally sampled disposal records from the following areas to determine whether certificates of disposal had been provided by the vendor and maintained by DTMB:

    - 43 of 56,648 retired equipment records from ITAM.

    - 68 of 74,999 disposal records from the AARP System. We randomly sampled 43 records from the full population and randomly selected 25 additional records from a judgmental subpopulation of 4,155 records where the pallet number field was blank.

    - 43 of 5,095 salvaged records from CMDB.

- Assessed the sufficiency of DTMB's process for ensuring that leased printers were effectively sanitized upon leaving the State's possession.

- Evaluated DTMB's manifest and pallet number creation processes for tracking IT equipment to be sent to the vendor for disposal. We also randomly sampled 4 of 37 manifests for review of completeness.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project our results to the respective populations.

OBJECTIVE #2

To assess the effectiveness of DTMB's efforts to prevent and detect the theft of surplus and salvage IT equipment.

To accomplish this objective, we:

- Randomly sampled 43 of 357 individuals with access to DTMB's building where surplus and salvage IT equipment is stored to evaluate for the principle of least privilege and proper authorization for building access.

- Observed the third-party vendor's process for picking up equipment from the Depot.

- Reviewed random samples of IT equipment inventory records from ITAM and CMDB that were marked lost, stolen, or missing to determine if equipment regularly went missing during the disposal process:

    - 28 of 275 ITAM inventory records.

    - 7 of 67 CMDB inventory records.

- Analyzed badge swipe access data from November 1, 2018 through August 6, 2019 for potentially suspicious patterns of employees accessing the building where surplus and salvage IT equipment was stored after normal working hours, on weekends, and on holidays.

- Tested physical security controls in place for untracked IT equipment by attempting to remove 6 smart phones from the surplus and salvage storage area and evaluating whether DTMB would detect the theft.

- Reviewed a random and judgmental sample of 36 hours of surveillance video to observe for suspicious activity from the 6 cameras in the surplus and salvage storage area. For each of the 6 cameras, we randomly sampled 3 of the 30 days from July 3, 2019 through August 1, 2019 with available footage. For each day, we judgmentally determined that we would randomly select 1 hour during normal working hours and 1 hour after normal working hours for a total of 2 of 24 hours for each sampled day.

- Performed a reconciliation of the IT equipment sent to the vendor for disposal with the payment received from the vendor for that equipment for the month of July 2018.

- Assessed segregation of duties* for users with elevated access rights to ITAM, CMDB, or the AARP System.

- Reviewed a selection of 21 hard drives and solid-state drives from an open bin in the surplus and salvage storage area. We scanned the drives using data recovery software to assess whether any confidential or sensitive files had been deleted but were still accessible.

- Reviewed a selection of 11 smart phones and non-Windows tablets from an open box in the surplus and salvage storage area. When possible, we manually reviewed the contents of the devices and scanned them using recovery software to assess whether any confidential or sensitive files were present.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. For our judgmental samples, we could not project our results to the respective populations.

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.

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 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 to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, 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.

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

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.
auditor's comments to agency preliminary response	Comments that the OAG includes in an audit report to comply with *Government Auditing Standards*. Auditors are required to evaluate the validity of the audited entity's response when it is inconsistent or in conflict with the findings, conclusions, or recommendations. If the auditors disagree with the response, they should explain in the report their reasons for disagreement.
Automated Asset Recovery Program (AARP) System	The system provided by DTMB to process State agency IT equipment disposal requests.
confidentiality	Protection of data from unauthorized disclosure.
Configuration Management Database (CMDB)	The system used by DTMB to inventory servers, stand-alone storage devices, and network equipment.
Depot	An area within a State-owned warehouse where surplus IT equipment is stored prior to disposal or redeployment.
disposal	Removal or release of media from organizational control following the decision that it does not contain sensitive data because the media never contained sensitive data or sanitization techniques were applied.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
Information Technology Asset Management System (ITAM)	The system used by DTMB to inventory desktop computers, laptop computers, and Windows tablets.
IT	information technology.
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. Our assessment of materiality is in relation to the respective audit objective.

media	Material on which data is or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
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.
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.
PII	personally identifiable information.
principle of least privilege	The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
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.
sanitization	A process that renders access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

segregation of duties	Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of his or her duties. Proper segregation of duties requires separating the duties of reporting, review and approval of reconciliations, and approval and control of documents.
SOM	State of Michigan.
threat	An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

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