STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

BROM STIBITZ
ACTING DIRECTOR

September 18, 2020

Mr. Richard Lowe, Chief Internal Auditor
Office of Internal Audit Services
Office of State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48933

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, as initially submitted on 3/27/2020, following is a summary table identifying our ongoing responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of IT Equipment Surplus and Salvage.

If you have any questions, or if we can be of further assistance, please don't hesitate to contact me directly.

Sincerely,

Signature Redacted

Brom Stibitz
Acting Director (Chief Deputy Director)
& Chief Information Officer
DTMB

Attachment: DTMB Corrective Action Plan Response to OAG IT Equipment Surplus and Salvage (071-0515-19)

CC: Senator Edward McBroom, Senate Oversight Committee
Representative Matt Hall, House Oversight Committee
Senator Roger Victory, Chair, Senate Appropriations Subcommittee on General Government
Representative Mark Huizenga, Chair, House Appropriations Subcommittee on General Government
Zack Kolodin, Executive Office of the Governor
Doug Ringler, Auditor General
Laura Clark, Acting Chief Security Officer

Jack Harris, Chief Technology Officer
Cindy Peruchietti, Director Agency Services
Eric Swanson, Director Center for Shared Solutions
Sherri Irwin, Director, Office of Support Services
Michelle Lange, Chief of Staff

DTMB

IT Equipment Salvage and Surplus

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB remediated: #2, #3, #6
2. Audit recommendations DTMB agreed with and remediation is in progress: #1, #4
3. Audit recommendations DTMB agreed with and is partially remediating: #5
4. Audit recommendations DTMB disagreed with: None

DTMB's Responses to Recommendations:

Finding #1 – Controls Needed to Ensure Sanitization and Disposal

DTMB agreed with the recommendation.

DTMB agreed 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 all devices assigned to a pallet are also assigned to a shipping manifest (January 2020).

DTMB agreed 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 (December 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 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.
    - The 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 State standard 1340.00.170.03.
- DTMB sanitizes physical server hard drives to DOD 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 State data is removed from storage media prior to disposal in accordance with State Technical Standard 1340.00.110.04. DTMB will continue to work with State 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 agreed with the recommendation and completed remediation.

DTMB updated its internal procedure to verify the vendor sanitization process (October 2019). DTMB now selects devices for verification after the 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

DTMB agreed with the recommendation and completed remediation.

DTMB updated its internal procedure to ensure 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).

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

DTMB agreed 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 continues to work with its vendors to establish a process to verify vendors' sanitization efforts are working as intended (anticipated completion October 2020).

Finding #5 – Improved Physical Security Controls Needed

DTMB agreed with the recommendation.

DTMB agreed 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 OAG's audit report DTMB began storing hard drives and loose media in locked bins in July 2019.

DTMB also agreed with the need to ensure access rights to the building are appropriate. DTMB established an internal procedure to review access rights and hours employees are allowed to access the building (January 2020). Additionally, DTMB utilizes existing processes to remove building access rights when appropriate.

DTMB agreed 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 would 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 established an internal procedure to review access rights and hours employees are allowed to access the building (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 agreed with the recommendation and completed remediation.

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