STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

MICHELLE LANGE
DIRECTOR

January 31, 2024

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 48913

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, part VII, 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 follow-up audit report of IT Equipment Surplus and Salvage (071-0515-19F).

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

Sincerely,

Michelle Lange

Michelle Lange
DTMB Director

c: Senator Sam Singh, Chair, Senate Oversight Committee
Senator Ed McBroom, Minority Vice Chair, Senate Oversight Committee
Senator John Cherry, Chair, Senate General Government Appropriations Subcommittee
Senator Thomas Albert, Minority Vice Chair, Senate General Government Appropriations Subcommittee
Representative Felicia Brabec, Chair, House General Government Appropriations Subcommittee
Representative Ann Bollin, Minority Vice Chair, House General Government Appropriations Subcommittee
Patti Tremblay, Executive Office of the Governor
Doug Ringler, Auditor General
Laura Clark, Chief Information Officer
Caleb Buhs, Chief Deputy Director
Sherri Irwin, Director of Office of Support Services, DTMB ICCO
Jayson Cavendish, Chief Security Officer
Heather Frick, Director Agency Services
Rex Menold, Chief Technology Officer
Eric Swanson, Director Center for Shared Solutions

Attachment

DTMB Corrective Action Plan
for the OAG's Follow-up Audit of IT Equipment Surplus and Salvage
(071-0515-19F)

Summary of Agency Responses to Recommendations

1. Audit finding DTMB partially agreed with and performed corrective action for that portion: 1b
2. Audit finding DTMB disagreed with and no further corrective action will be performed: 5a

DTMB Responses to Recommendations

Finding #1 – Controls Needed to Ensure Sanitization and Disposal

Finding 1, Subpart 1b

DTMB disagrees with the need to establish additional procedures related to whether a device contains a hard drive or stored data. The processes implemented by the State of Michigan reduce the risk to an acceptable level or do not necessitate the development of such a process as the risk is not applicable.

The State computers, laptops, and tablets are encrypted at the hardware level which prevents accessing data even if the hard drive is separated and accessed by another device; this reduces the risk to an acceptable level.

DTMB agrees DTMB did not always receive the certificates from the vendor within 30 days of equipment pickup as required in the contract. DTMB reviewed and updated contract language for the vendor to provide equipment sanitization certificates (December 2023).

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:05 PM)

SOM Technical Standard 1340.00.110.01 states, when required based on data classification, the organization tracks, documents, and verifies media sanitization and disposal. Without procedures to determine whether devices contain hard drives or stored data, DTMB cannot ensure compliance with this Standard. While DTMB asserts the devices are encrypted, the Standard does not eliminate or change the requirement based on whether or not devices are encrypted.

Finding #5 – Improved Physical Security Controls Needed

Finding 5, Subpart 5a

DTMB disagrees with the need to further restrict access to the building beyond the existing restrictions and processes which are in place. As DTMB noted in the prior audit response, the cost to restrict the access to the Surplus and Salvage area of the building beyond general building access would exceed the cost benefit of doing so.

DTMB implements the following controls to reduce risk to an acceptable level:

- The building itself is secured by gates, security guards, and the need to use an access card to enter the building. DTMB restricts the access to the building to individuals who have a business need to access the building for their job responsibilities.
- The State computers, laptops, and tablets are encrypted at the hardware level which prevents accessing data even if the hard drive is separated and accessed by another device; this reduces the risk to an acceptable level.
- Additionally, State network infrastructure devices (routers, switches, firewalls) do not possess internal data storage. Furthermore, as part of a separate secure disposal process, the hard drives from servers hosted in the State's hosting center are sanitized and shredded.
- 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.
- As noted in the OAG's audit report, DTMB secures smart devices, hard drives, and loose media in locked bins.
- Visitors are escorted within the building.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:05 PM)

This statement is misleading as DTMB's decision to assume the risk does not align with its own SOM Technical Standard 1340.00.110.01.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:05 PM)

SOM Technical Standard 1340.00.110.01 states agencies are to physically control and securely store digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded or contained on it and protects this media until it is destroyed or sanitized. The Standard does not eliminate this requirement based on whether or not devices are encrypted.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:05 PM)

Laptops, PCs, and other larger devices which may contain confidential information are stacked on pallets, unsecured in the salvage area of the warehouse.