Office of the Auditor General

Performance Audit Report

Security of Mobile Devices

Department of Technology, Management, and Budget

August 2024

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

171-0555-24

> 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

Security of Mobile Devices

Department of Technology, Management, and Budget (DTMB)

Report Number:
171-0555-24

Released:
August 2024

Data security in a mobile device environment is critical to data protection. Mobile devices, including smartphones and tablet computers, have computing power equivalent to traditional personal computers but with the convenience of portability which enables users to access and store confidential and sensitive information. The DTMB Smart Device Support Team (SDST) is responsible for DTMB's administration of mobile devices, which includes designing, implementing, and enforcing device configurations. As of March 18, 2024, the SDST administered over 23,000 mobile devices.

Audit Objective	Conclusion
Objective 1: To assess the sufficiency of DTMB's efforts to administer the secure configuration of mobile devices.	Sufficient, with exceptions

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB needs to ensure State owned and managed mobile devices are configured in accordance with best practices to reduce risks to the devices and State of Michigan data (Finding 1).	X		Partially agrees
DTMB did not document approval for device access to blocked Internet locations to ensure it was appropriate, reasonable, and sufficiently restricted to potentially high-risk Internet locations (Finding 2).		X	Agrees

Audit Objective	Conclusion
Objective 2: To assess the effectiveness of DTMB's efforts to establish a governance structure over mobile device security.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Mobile device configuration management controls need improvement to sufficiently protect the State's mobile devices from threats, vulnerabilities, and loss of State information (Finding 3).	X		Partially agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB should strengthen its processes to restrict access to unauthorized mobile applications (Finding 4).		X	Disagrees
DTMB did not enforce the installation of a mobile threat defense solution on all managed mobile devices (Finding 5).		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

August 13, 2024

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Director Lange and Chief Information Officer Clark:

This is our performance audit report on the Security of Mobile Devices, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency provided the 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

SECURITY OF MOBILE DEVICES

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SECURITY CONFIGURATION OF MOBILE DEVICES

BACKGROUND

The configuration* of a system and its components have a direct impact on its security* posture. How the configurations are established and maintained requires a disciplined approach for providing adequate security.

The Department of Technology, Management, and Budget (DTMB) Smart Device Support Team (SDST) is primarily responsible for the secure configuration of mobile devices. SDST utilizes a mobile device manager* (MDM) to enroll, configure, and actively manage mobile devices. The MDM solution manages user access to State resources and simplifies application and device management across many devices. It also facilitates configuration management* which includes pushing updates, settings, and restrictions to the devices and enables DTMB to establish requirements via compliance policies which devices must meet to access State resources.

The mobile threat defense* (MTD) solution monitors the ongoing behavior of mobile devices within the current environment and allows for functionality such as blocking known malicious Uniform Resource Locators* (URLs) or phishing sites. Also, the MTD provides continuous monitoring for assessing the risk of applications downloaded to a mobile device and can block network traffic and detect network-based attacks in real time.

AUDIT OBJECTIVE

To assess the sufficiency of DTMB's efforts to administer the secure configuration of mobile devices.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- Configuration settings in the MTD were generally secure.

- DTMB properly handled lost and stolen device reports and device retirement requests to ensure the security of mobile devices.

- Material condition* related to configuring mobile devices in accordance with best practices and State of Michigan (SOM) technical standards (Finding 1).

- Reportable condition* related to the lack of approvals for allowing blocked Internet locations (Finding 2).

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

FINDING 1

Configure mobile devices in accordance with best practices and SOM technical standards.

DTMB did not fully ensure State owned and managed* mobile devices were configured in accordance with best practices and SOM technical standards. Proper configurations reduce the risk of compromise to the State's mobile devices and data, thereby protecting them from unauthorized modification, loss, or disclosure.

The MDM solution manages user access to State resources, simplifies application and device management, and allows for configuration management, including pushing updates, settings, and restrictions, to the devices. Also, the solution enables DTMB to establish requirements via compliance policies, which devices must meet to access State resources. Approximately 99.8% of managed mobile devices are State owned.

SOM Technical Standard 1340.00.060.01 requires DTMB to establish, document, and implement configuration settings for IT products employed within the information system using security configuration checklists which reflect the most restrictive mode consistent with operational requirements. According to the National Institute of Standards and Technology* (NIST), common secure configurations provide recognized, standardized, and established benchmarks stipulating secure configuration settings for IT products and platforms as well as instructions for configuring those products or platforms to meet operational requirements.

We reviewed State owned and managed mobile devices and determined DTMB did not:

a. Configure several mobile device restrictions recommended by best practice guidance.

   We compared DTMB's MDM configurations and compliance policies with Center for Internet Security* benchmarks and noted several deviations from recommended configurations, including a configuration to immediately restrict access to State resources when a device becomes noncompliant.

   Although we referenced Center for Internet Security benchmarks for our comparison, according to NIST Special Publication 800-124, an enterprise may reference suggested secure mobile device configuration guidance from any established entity providing it.

b. Restrict the use of removable media on mobile devices as required by SOM technical standards.

   SOM Technical Standard 1340.00.110.01 requires information system owners to restrict the use of certain

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

media on mobile devices. Information system media includes digital media such as flash drives and external hard disk drives.

DTMB did not compare configurations impacting mobile devices with best practices.

DTMB informed us it did not benchmark its MDM configurations against best practices. Instead, it used guidance from the MDM vendor and internal and external subject matter experts to create the initial configurations when the MDM was adopted in 2017.

We consider this finding to be a material condition because of the number of configurations deviating from best practice guidance.

RECOMMENDATION

We recommend DTMB configure State owned and managed mobile devices in accordance with best practices and SOM technical standards.

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 1 are presented on page 20.

FINDING 2

Lack of approvals for allowing blocked Internet locations.

DTMB did not document approval for device access to blocked Internet locations. Without this approval, DTMB cannot determine whether access is appropriate, reasonable, and sufficiently restricted to potentially high-risk locations.

DTMB utilizes URL filtering tools, including the MTD, to block certain locations. Users with a verified business need to access blocked locations must submit an agency approved form to DTMB. Based on a security review of the site, the DTMB Michigan Security Operations Center may approve access.

SOM Technical Standard 1340.00.060.01 requires DTMB to identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.

We selected 7 MTD blocked locations, subsequently allowed by DTMB, and requested the corresponding approval form. DTMB could not provide approval forms for all 7 (100%) of these allowed locations.

DTMB indicated it did not consistently document user request details allowing it to trace the allowed location back to its respective approval form. Also, DTMB informed us many allowed locations were carried forward from other URL filtering platforms during the implementation of the MTD.

RECOMMENDATION

We recommend DTMB document approval for device access to blocked Internet locations.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees it did not always document a reference to the agency-approved request within the system used to enable access to sanctioned sites. DTMB has implemented a process to include a reference to the agency-approved request within the system used to enable access to the sanctioned site.

GOVERNANCE STRUCTURE OVER MOBILE DEVICE SECURITY

BACKGROUND

IT governance is the leadership, structures, and processes which enable an organization to achieve its strategies and objectives. According to the IT Governance Institute* (ITGI), IT management should focus on making the organization more effective, increasing operational efficiencies, decreasing costs, and managing risks associated with security, reliability, and compliance.

SDST is primarily responsible for governance over State mobile devices and for ensuring the implementation of and compliance with SOM policies, standards, and procedures. Other areas within DTMB may also be involved depending on the policy, standard, or procedure.

When risks are unable to be sufficiently mitigated to conform with DTMB policies, standards, procedures, processes, and best practices, then business processes take priority and formal exceptions should be sought. These exceptions are submitted, reviewed, and approved by the Executive Technology Review Board (ETRB).

AUDIT OBJECTIVE

To assess the effectiveness* of DTMB's efforts to establish a governance structure over mobile device security.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Users with access to the MDM and MTD were reasonable.
- ETRB approval existed to exempt an agency from MTD settings.
- SDST implemented an effective process to approve nonstandard mobile devices prior to MDM enrollment.
- Implemented requests for changes were documented, tested, and approved.
- Material condition related to establishing and implementing effective configuration management controls for mobile devices (Finding 3).
- Two reportable conditions related to strengthening processes to restrict access to applications and approvals for MTD exclusions (Findings 4 and 5).

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

FINDING 3

Mobile device configuration management controls needed.

DTMB had not fully established and implemented configuration management controls for mobile devices. These controls directly impact DTMB's ability to protect the State's mobile devices from threats*, vulnerabilities*, and loss of information.

Our review of DTMB's mobile device configuration management determined DTMB did not:

a. Document baseline configurations for mobile devices. These configurations define specifications required for mobile devices and mobile device configuration items such as MTD and MDM solutions.

   SOM Technical Standard 1340.00.060.01 requires DTMB to develop, document, and maintain a current baseline configuration. NIST Special Publication 800-53 states baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems.

   DTMB informed us it considered the actual configurations within the solutions to be the baseline configurations. DTMB also did not determine the applicability of the configuration management standard to mobile devices and was not aware it needed to document baselines.

b. Use security configuration checklists to establish configuration baselines. Using checklists would help ensure the baselines are in line with best practices while meeting operational requirements.

   SOM Technical Standard 1340.00.060.01 requires DTMB to establish and document configuration settings for IT products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements. NIST Special Publication 800-53 states the configuration settings from security configuration checklists become part of the baseline configuration.

   DTMB informed us it used guidance from the MDM vendor, internal and external subject matter experts, and departmental requests to establish the baseline configurations.

c. Establish a formal process to review and update baseline configurations for mobile devices. Formalized processes would help to ensure mobile devices remain secure and configurations remain consistent with industry best practices.

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

SOM Technical Standard 1340.00.060.01 states baseline configurations should be reviewed and updated:

- According to the system's configuration management program, but no less than every 365 days.

- When required because of a major system change or upgrade.

- As an integral part of upgrades.

DTMB informed us baseline configuration updates were performed in response to alerts from vendors, patch release notes, research from internal and external subject matter experts, and departmental requests. We determined DTMB had a formal process to implement changes; however, this process did not include all updates, systematic timely reviews, and the determination of updates as revisions to baselines.

DTMB did not have a configuration management plan.

d. Develop a configuration management plan for mobile devices. SOM Technical Standard 1340.00.060.01 requires DTMB to develop, document, and implement a configuration management plan which:

- Addresses roles, responsibilities, and configuration management processes and procedures.

- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration items.

- Defines the configuration items for the information system and places these items under configuration management.

DTMB did not determine the applicability of the configuration management standard. Although DTMB had formally addressed some configuration activities, it had not developed an overall configuration management plan to cover all aspects of securing mobile devices, including parts a. through c. of this finding. As DTMB refines its plan, it should implement controls to protect the plan from unauthorized disclosure and modification.

We consider this finding to be a material condition because of the number of weaknesses identified and the importance of the controls which ensure the secure configuration of mobile devices.

RECOMMENDATION

We recommend DTMB fully establish and implement configuration management controls for mobile devices.

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 3 are presented on page 21.

FINDING 4

Strengthen processes to restrict access to applications.

DTMB should strengthen its processes to restrict access to unauthorized mobile applications. Allowing users to install applications not explicitly approved by DTMB could introduce malicious applications designed to exfiltrate information by a user.

NIST Special Publication 800-53 suggests organizations employ a deny-all, allow-by-exception policy to allow the execution of authorized software programs on the information system. Also, NIST Special Publication 800-124 suggests limiting access to only approved app stores* or restricting which applications may be installed.

DTMB maintains an enterprise mobile app store of approved applications. However, users can sign in to other mobile app stores and download potentially unapproved, risky applications. Also, some unapproved applications are preinstalled from the manufacturer and cannot be removed, according to DTMB.

Our review of the MDM, MTD, and applications installed on managed mobile devices identified devices with installed risky applications. State information could be backed up to these applications and pose a greater risk because the mechanisms the State uses to protect its data are no longer present. DTMB asserted controls are in place at the network level to block traffic to and from prohibited applications and websites; however, testing of the implementation of these network-level controls was outside of the scope of this audit.

DTMB began implementing projects to evaluate mobile application management and protection policies through the MDM, which would limit mobile devices to install only authorized applications. However, DTMB delayed these projects until it refined its review and approval process. Also, according to DTMB, it is working on an adjustment to the device enrollment process which would remove unapproved pre-installed applications.

RECOMMENDATION

We recommend DTMB strengthen its processes to restrict access to unauthorized mobile applications.

AGENCY PRELIMINARY RESPONSE

DTMB disagrees. Given the length of DTMB's preliminary response, the response and our auditor's comments to Finding 4 are presented on page 23.

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

FINDING 5

Approvals needed for MTD solution exclusions.

DTMB did not ensure approvals existed to exclude entities from the MTD requirement. Mobile devices without the MTD solution are more vulnerable to malicious applications, network-based attacks, phishing attacks, improper configurations, and known vulnerabilities in mobile apps or the mobile operating system* (OS) itself.

SOM Technical Standard 1340.00.020.01 requires the establishment of usage restrictions, configuration requirements, connection requirements, and implementation guidance for system owner-controlled mobile devices. This includes implementation of mandatory protective software (e.g., malicious code detection and firewall), scanning devices for malicious code, and updating virus protection software.

SOM Technical Standard 1305.00.02 requires any exception to approved technical policies or standards be approved by ETRB.

We determined two entities were excluded from the MTD requirement, and neither entity had ETRB approval for its exclusion. One entity had a temporary exclusion while evaluating its compliance with federal requirements, and the other, according to DTMB, was excluded based solely on a verbal agreement.

RECOMMENDATION

We recommend DTMB ensure approvals exist to exclude entities from the MTD requirement.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees approved exceptions were not documented. DTMB will obtain temporary exceptions (September 2024) while DTMB and the entities pilot the service to determine if the service is compatible with their business needs. At the end of the pilot (April 2025), the DTMB will either deploy the service to applicable users or renew the exception to reflect an ongoing Agency business need (November 2025).

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

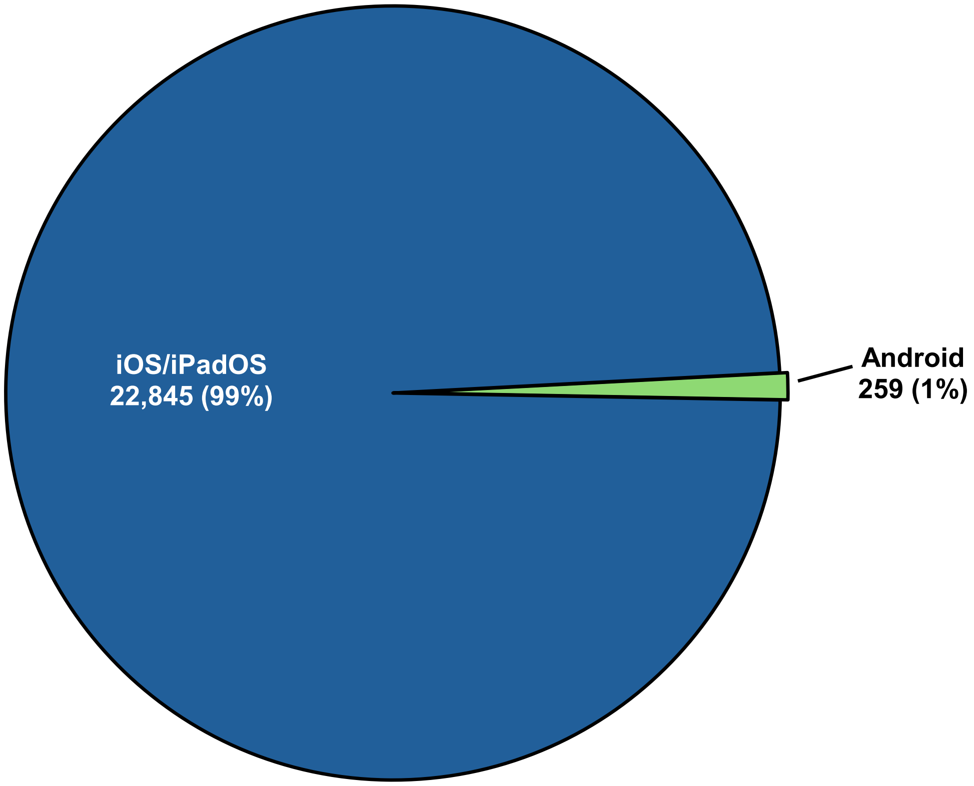
SUPPLEMENTAL INFORMATION

UNAUDITED
Exhibit 1

SECURITY OF MOBILE DEVICES
Department of Technology, Management, and Budget

Mobile Devices by Operating System

Count of mobile devices by operating system (OS) able to connect to State resources as of March 18, 2024:



Source: The OAG prepared this exhibit using information received from MDM.

UNAUDITED
Exhibit 2

SECURITY OF MOBILE DEVICES
Department of Technology, Management, and Budget

Mobile Devices Connecting to State Resources by Entity

	Number of Mobile Devices as of		Percent
Entity	March 18, 2024	July 1, 2014	Change
Michigan Department Health and Human Services	6,596	4,545	45%
Michigan Department of State Police	3,286	1,298	153%
Michigan Department of Transportation	2,265	1,568	44%
Michigan Department of Corrections	1,698	542	213%
Department of Technology, Management, and Budget	1,652	1,207	37%
Department of Environment, Great Lakes, and Energy	1,401	238	489%
Department of Natural Resources	1,175	277	324%
Department of Labor and Economic Opportunity	1,028	0	N/A
Department of Licensing and Regulatory Affairs	933	614	52%
Michigan Department of Agriculture and Rural Development	448	280	60%
Department of Treasury	422	318	33%
Department of Attorney General	376	88	327%
Michigan Lifelong Education, Advancement, and Potential	249	0	N/A
Other Entities*	237	38	524%
Michigan Department of State	230	65	254%
Michigan Department of Education	209	306	(32%)
Department of Military and Veterans Affairs	202	53	281%
Department of Insurance and Financial Services	181	66	174%
Bureau of State Lottery	109	0	N/A
Unemployment Insurance Agency	108	0	N/A
Michigan State Housing Development Authority	104	0	N/A
Michigan Civil Service Commission	80	0	N/A
Michigan Gaming Control Board	76	0	N/A
Department of Civil Rights	39	22	77%
Total	23,104	11,525	
Number of increase from prior audit	11,579		
Percentage increase from prior audit	100%		

* Other Entities include the Center for Educational Performance and Information, Michigan Independent Citizens Redistricting Commission, Michigan Strategic Fund - Office of the Chief Compliance Officer, Executive Office of the Governor, Office of the State Employer, and other mobile devices which did not have an identifiable entity.

N/A = Not applicable.

Source: The OAG prepared this exhibit using information received from MDM.

Finding 1 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 1 and our auditor's comments providing further clarification and context where necessary.

Finding 1: Configure mobile devices in accordance with best practices and SOM technical standards.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE

DTMB partially agrees.

For subpart a., DTMB disagrees. DTMB does not use the Center for Internet Security (CIS) benchmarks for configuration management of mobile devices, nor is the State required to use those benchmarks. Therefore, a full comparison to these benchmarks is not appropriate from DTMB's perspective.

As a result of the varying needs of State agencies and diverse configuration requirements a "one size fits all" MDM policy isn't tenable, and it is important to note that implementing all the recommendations from an external benchmark would likely render some systems inoperable for many business functions.

The State of Michigan (SOM) Technical Standard 1340.00.060.01 requires that DTMB "establishes and documents configuration settings for information technology products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements" but does not mandate the implementation of an external or published checklist. The SOM Standard is met through a combination of enterprise-wide change control processes and system specific Standard Operating Procedures (SOP). The configurations are based on intentional decision-making by DTMB IT management and technical personnel to enable the system to run and meet state business needs. This includes vendor recommendations, discussion with subject-matter experts, and input from DTMB's Cybersecurity & Infrastructure Protection division. This meets the requirements presented in the Technical Standard as the configuration baseline and checklist is completed and documented for each endpoint through automated processes.

For subpart b., DTMB agrees. DTMB has initiated the process to implement technical restrictions on the use of removable media on mobile devices as appropriate for the SOM environment. DTMB expects the technical restriction will be implemented by October 2024. DTMB has IT policies, standards, and procedures to promote the acceptable use of IT resources, including mobile devices to safeguard state information and systems. Agency and SOM staff are required to follow these policies, standards, and procedures to safeguard state data. Annual SOM IT cybersecurity training also ensures staff are aware of state policies and cybersecurity best practices.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE

DTMB did not provide evidence as to the benchmarking of configurations to any best practices. Nor did it provide documented processes specifying its "intentional decisions" and approvals when tailoring configurations which deviated from best practices. We utilized the CIS benchmarks since these are known industry best practices and recommended by NIST, of which, the SOM technical Standards are derived.

Our comparative review identified high-risk configurations which could compromise SOM resources. One such configuration was DTMB's assertion it immediately restricted noncompliant devices from State resources, as recommended by CIS. However, this did not match DTMB's MDM setting. To protect the confidentiality of this information, we separately notified DTMB of similar settings.

The SOM technical standard states the configuration settings should reflect the most restrictive mode consistent with operational requirements. DTMB states it could not implement all recommendations because some systems would be inoperable. Although it may be true to an extent, DTMB did not use any benchmarks because had it done so, it would have documented the rationale for the configuration deviations.

DTMB did not provide evidence of a Standard Operating Procedure encompassing a methodology to benchmark configurations.

DTMB's own response to Finding 3, subpart c., indicates it is writing a Standard Operating Procedure, which defines an annual review of configurations.

DTMB did not provide evidence that enterprise-wide change control support encompassed all configurations as noted with Finding 3, subpart c.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 1

Go to Finding 2

Finding 3 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 3 and our auditor's comments providing further clarification and context where necessary.

Finding 3: Mobile device configuration management controls needed.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
DTMB partially agrees.	
For subpart a., DTMB disagrees it did not document baseline configurations for mobile devices. DTMB documents and enforces technical baseline configurations within the system, as opposed to documenting them in a separate external document. DTMB's process is considered a technical control, which is stronger than an administrative control (i.e., a paper document listing the baseline configurations).	SOM technical standards require "documented" configuration baselines, as recommended by NIST. Configurations within the system are subject to user alteration, void considerations, lack the rationale on formal approvals for established exclusions, lack easily identifiable historical settings, and are unobtainable with any system downtime.
DTMB meets the SOM Technical Standard which requires DTMB "develops, documents, and maintains under configuration control, a current baseline configuration of the information system" by utilizing an enterprise-wide Request For Change (RFC) process which logs changes to configurations including rollback procedures.	DTMB did not provide evidence that an enterprise-wide change control support encompassed all configurations as noted with subpart c. of this Finding and our auditor's comments to Finding 1, subpart a.
Additionally, changes both within and outside the RFC process are documented within DTMB's Ticket and Service Management system. Finally, the configurations stored within the system include an audit log that can be reviewed on an as needed basis.	Ticket management systems and logs, like system configurations, are absent consideration, lack approval for omissions, and are not easily searchable.
For subpart b., DTMB partially agrees. SOM Technical Standard 1340.00.060.01 requires the use of configuration checklists that ensure security controls are assigned to each SOM endpoint device but does not mandate the implementation of an externally sourced or published checklist, nor does it require that the checklist be stored outside of the system.	According to NIST, common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, and security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. SOM technical standards require "documented" security configuration checklists, as recommended by NIST. A checklist within the system would be subject to the same risks as noted in our auditor's comments to subpart a of this Finding.
The DTMB Smart Device Support Team's process for creating endpoint configuration checklists appropriate for the SOM environment includes intentional decision-making by DTMB IT management and technical personnel, vendor recommendations, discussion with subject-matter experts, and input from DTMB's Cybersecurity & Infrastructure Protection division to enable the system to meet state business needs and operational requirements.	DTMB's intentional decision-making did not include the documented configuration checklists required by SOM Technical Standard 1340.00.060.01 or a formal review and indication as to why this portion of the Standard might not be applicable.
DTMB's endpoint checklist is contained within the Mobile Device Management (MDM) system, and the deployment and verification of these configuration items are automated using the same tool. This meets the requirements presented in the SOM Technical Standard as the configuration checklist is completed and documented for each endpoint through automated processes.	See our auditor's comments at the beginning of subpart b. of this Finding.

Continued on next page.

DTMB is evaluating the use of an appropriate external benchmark as an additional input to the existing process of identifying applicable configuration items included in the existing endpoint configuration checklist. DTMB anticipates the evaluation will be completed in September 2024. DTMB is also developing a SOP that will govern implementation of deviations from the baseline contained within the system to ensure they are approved through DTMB's established exception processes. DTMB anticipates this SOP will be completed in October 2024.

For subpart c., while DTMB did not document a formal internal procedure to review and update baseline configurations for mobile devices on an annual basis, it reviews configurations as part of ongoing operational processes. The change controls adhere to both enterprise-wide and internal procedures that prescribe how updates to the baseline configurations are to be made and recorded, and also describe the specific cadence on which configurations are to be updated.

While SOM 1340.00.060.01 does not require a formal procedure for reviewing and updating baseline configurations, DTMB is writing a SOP that defines an annual review of configurations that have not been modified or considered for modification in the preceding year. DTMB anticipates the internal procedure will be completed in September 2024.

For subpart d., DTMB disagrees DTMB did not develop a *standalone configuration management plan for mobile devices. Mobile devices follow the configuration management plan and processes which are documented and managed by internal SOPs and the enterprise-wide service request for changes process which addresses roles, responsibilities, and configuration management processes and procedures. The DTMB Smart Device Support Team reviews configurations as part of ongoing operational processes and adheres to applicable DTMB requirements; the configuration items for the information system are defined within the system and are governed by the configuration procedures referenced in this response. The configuration management plan is protected from unauthorized disclosure and modification by both technical and administrative controls.*

DTMB indicated it is evaluating the addition of a self-selected external benchmark. Therefore, it is unclear why DTMB disagrees with Finding 1, which recommends configuring mobile devices in accordance with best practices.

As noted in the Finding, DTMB's process neglected to include systematic timely reviews, all available updates, or a determination by DTMB on if the updates warranted revisions to the baseline configurations. The SOM Technical Standard 1340.00.060.01 is clear and requires a formal process for reviewing and updating baseline configurations for mobile devices.

DTMB's operational processes were not comprehensive. It did not provide evidence of an overall review and its own response to subpart c. of this Finding specifies DTMB is creating a Standard Operating Procedure to annually review configurations.

DTMB did not provide evidence that enterprise-wide change control support encompassed all configurations as noted with subpart c. of this Finding.

Although DTMB may strive to protect a theoretical configuration management plan, until it is formalized and tangible, DTMB cannot make assurances it is protected from unauthorized disclosure and modification.

We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 3

Go to Finding 4

Finding 4 Agency Preliminary Response and Auditor's Comments to Agency Preliminary Response

This section contains DTMB's preliminary response to Finding 4 and our auditor's comments providing further clarification and context where necessary.

Finding 4: Strengthen processes to restrict access to applications.

DTMB provided us with the following response:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
DTMB disagrees. While DTMB has not implemented a technical control to prevent users from installing applications from unmanaged mobile application stores, DTMB has implemented controls to mitigate the risks inherent with conducting business in digital environments, which includes the use of mobile devices for official State work. Such controls include application sandboxing, conditional access policies enforcement, and blocking access to specific websites and applications both at the device and network levels.	DTMB's technical controls are not all-inclusive since some entities do not have application management controls (Finding 5) and noncompliant devices are not immediately restricted from SOM data (Finding 1).
Beyond the various technical controls, SOM personnel are required to follow policies, standards, and procedures that guide users to responsible data management, device usage, and the acceptable use of mobile applications to safeguard information and systems. Examples of this are the State of Michigan's Acceptable Use Standard which governs acceptable use of state resources and data by SOM employees, and the SOM Social Media Guidelines standard. Lastly, the State of Michigan directs users to complete cybersecurity awareness training on an ongoing basis to ensure staff are aware of applicable policies and cybersecurity best practices.	DTMB self-identified the need to restrict app store accessibility as noted in this Finding. Restricting access to other mobile app stores is an immediate and primary control. Policies, standards, procedures, and training may mitigate risk; however, these are secondary controls. The current process puts SOM data at risk.
While restricting access to public app stores would further reduce risk beyond the requirements of applicable SOM standards, the above controls and provisions have reduced the risk identified to an acceptable level.	We considered the agency response and based on our comments above, the finding stands as written.

Go Back to Finding 4

Go to Finding 5

DESCRIPTION

A mobile device is a portable computing device with a small form factor resulting in it being easily carried by a single individual. The devices are designed to operate without a physical connection; possess local, nonremovable data storage; and are powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors to allow the device to capture information (photograph, video, record, or determine location), built-in-features for synchronizing local data with remote locations, and capabilities to run applications to expand the device's basic functionality. Mobile devices primarily include mobile phones and tablets utilizing mobile OSs such as iOS and Android.

DTMB uses an MDM solution to manage the State employees' use of mobile devices. An MDM solution allows DTMB to enroll, configure, and actively manage mobile devices and offers mobile application management, as well as the ability to sync to DTMB's MTD solution.

SDST acts as the support center for State mobile device users by assisting with user submitted help desk requests. Help desk requests range from a variety of issues such as device enrollment, troubleshooting, device lockouts, reports of lost/stolen devices, device retirement requests, and more.

State employees use mobile devices to perform work-related functions, to facilitate work when in meetings or traveling, and to access the State's IT resources, such as e-mail, applications, and information systems. As of March 18, 2024, approximately 23,000 mobile devices could connect to State resources.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the records and processes related to security configuration and governance over mobile devices. 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 scope did not include the administration of mobile devices within the legislative and judicial branches of State government. Also, in December 2023, during our audit fieldwork, DTMB migrated to a new MTD, which we did not include in our scope. In addition, we did not obtain a mobile device to determine how configured restrictions functioned on a managed mobile device and we excluded controls over mobile device procurement and disposal.

As part of the audit, we considered the five components of internal control* (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2022 through March 18, 2024.

METHODOLOGY

We conducted a preliminary survey of controls over mobile devices, including configuration controls, access controls*, and governance structure. During our preliminary survey, we:

- Interviewed DTMB management and staff to obtain an understanding of how mobile devices are managed and secured.

- Reviewed SOM policies, standards, procedures, and industry best practices related to mobile device security.

- Gained an understanding of existing SOM policy exceptions for mobile devices and the process to request and approve exceptions from SOM policy.

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

- Assessed DTMB's process to monitor mobile device event logs from the MDM and MTD.

- Obtained an understanding of SDST's change control process and the types of changes subject to change controls.

OBJECTIVE 1

To assess the sufficiency of DTMB's efforts to administer the secure configuration of mobile devices.

To accomplish our first audit objective, we:

- Compared established configurations in DTMB's MDM with industry best practices.

- Randomly and judgmentally sampled 7 of 672 blocked Internet locations from 6 of 19 different profiles as of October 16, 2023 to determine if configurations were set correctly for select MTD settings.

- Reviewed 2,000 help desk tickets and MDM information from June 12, 2023 through October 18, 2023 to assess DTMB's handling of mobile device requests. Specifically, we randomly sampled:

    - 16 of 158 identified mobile device retirement requests.

    - 10 of 49 identified lost and stolen mobile device requests.

- Reviewed an additional 526 help desk tickets from January 2024 and assessed DTMB's handling of all 20 tickets related to lost and stolen mobile devices.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk; therefore, we could not project the results to the respective populations.

OBJECTIVE 2

To assess the effectiveness of DTMB's efforts to establish a governance structure over mobile device security.

To accomplish our second audit objective, we:

- Tested a random sample of ETRB approvals for 25 of 356 nonstandard mobile device MDM enrollments as of March 12, 2024.

- Reviewed ETRB approval relating to the configuration of an MTD setting.

- Reviewed the change process phases from October 1, 2022 through October 1, 2023 and randomly sampled 2 of the 15 system changes for completeness, documentation, and approvals.

- Compared mobile device listings between the MDM and MTD as of October 2023 to determine if the MTD was installed on all managed mobile devices. We judgmentally selected 10 of 86 mobile devices without MTD installed to determine the reasonableness of the MTD not being installed on the device.

- Tested appropriateness of access for all 10 individuals with access to the MTD as of September 20, 2023 by tracing access levels to the user's respective job functions and determined if users were current State employees.

- Randomly and judgmentally sampled 25 (10%) of 248 users with MDM access as of September 20, 2023 to determine reasonableness based on job function and if the users were still State employees.

- Analyzed applications as of November 6, 2023 and determined if prohibited applications or applications exhibiting risky behavior were installed on managed mobile devices.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk; therefore, we could not project the results to the respective populations.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material 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.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality* of configurations applicable to mobile devices, we summarized our testing results for presentation in the report and provided the underlying details for all of the findings to DTMB management.

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

AGENCY RESPONSES

Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates it agrees with 2 of the recommendations, partially agrees with 2 of the recommendations, and disagrees with 1 recommendation.

The agency preliminary response following 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.

PRIOR AUDIT FOLLOW-UP

The findings and recommendations from our prior performance audit of Data Security Using Mobile Devices, DTMB, issued in January 2015 (071-0555-14), were not significant within the context of our current audit objectives.

SUPPLEMENTAL INFORMATION

Our audit report includes supplemental information presented as Exhibits 1 and 2. Our audit was not directed toward expressing a conclusion on this information.

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.

app store
An online portal through which software programs are made available for purchase and download for mobile devices.

auditor's comments to agency preliminary response
Comments 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.

Center for Internet Security
A not-for-profit organization establishing and promoting the use of consensus-based best practice standards to raise the level of security and privacy in IT systems.

confidentiality
Protection of data from unauthorized disclosure.

configuration
The way a system is set up. Configuration can refer to either hardware or software or the combination of both.

configuration management
The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

DTMB
Department of Technology, Management, and Budget.

effectiveness
Success in achieving mission and goals.

ETRB
Executive Technology Review Board.

internal control
The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.

IT

information technology.

IT Governance Institute (ITGI)

A research think tank that is a leading resource on IT governance for the global business community. ITGI aims to benefit enterprises by assisting enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. By conducting original research on IT governance and related topics, ITGI helps enterprise leaders understand and have the tools to ensure effective governance of IT within their enterprise.

managed

Enrolled in the MDM.

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.

mobile device manager (MDM)

Used to deploy, configure, and actively manage mobile devices.

mobile threat defense (MTD)

Solution monitoring for known threats, vulnerabilities, and compromised or malicious applications and websites. The MTD gathers data and helps analyze threats to devices in an enterprise environment. It monitors the OS and information about apps and network connections and provides data to the solution which it uses to identify suspicious or malicious behavior.

National Institute of Standards and Technology (NIST)

An agency of the U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum-security requirements for federal programs.

operating system (OS)

A computer program, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an OS is to provide an environment in which a user can execute applications.

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.

reportable condition A matter, in the auditor's judgment, less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.

SDST DTMB Smart Device Support Team.

security Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

SOM State of Michigan.

threat An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

Uniform Resource Locator (URL) A reference to a resource which specifies its location on a computer network and a mechanism for retrieving it. Also known as an address on the web.

vulnerability Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070