MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

DATA SECURITY USING MOBILE DEVICES

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

January 2015

Doug A. Ringler, CPA, CIA
AUDITOR GENERAL

071-0555-14

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
http://audgen.michigan.gov

OAG
Office of the Auditor General

Report Summary

Performance Audit

Data Security Using Mobile Devices

Department of Technology, Management, and Budget

Report Number:
071-0555-14

Released:
January 2015

Data security in a mobile device environment is critical to data protection because mobile devices, including smartphones and tablets, have computing power equivalent to traditional personal computers and enable users to access and store confidential and sensitive information on their mobile devices. Between June 1, 2014 and July 1, 2014, over 11,500 mobile devices connected to the State's information technology (IT) resources. The Department of Technology, Management, and Budget (DTMB) Smart Device Support Team is responsible for configuring and managing mobile devices. In addition, DTMB Cybersecurity and Infrastructure Protection is responsible for oversight of security issues associated with the State's assets, systems, and networks, including mobile devices.

Audit Objective	Audit Conclusion
Objective 1: To assess the effectiveness of DTMB's efforts to establish a governance structure and provide guidance regarding mobile device security.	Moderately effective

Finding Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not fully established an effective governance structure over the security of mobile devices. Necessary improvements include the establishment of roles and responsibilities for mobile device security, an acceptable method for removing data from devices, and other policies and guidance (Finding 1).		X	Agrees

Audit Objective	Audit Conclusion
Objective 2: To assess the effectiveness of DTMB's efforts to design, implement, and enforce the secure configuration of mobile devices.	Not effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not enforce security configuration profiles within the State's Mobile Device Management (MDM) System. Over 1,900 (16.8%) devices were not managed by the State's MDM System (Finding 2).	X		Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not fully established effective security configurations for mobile devices. We noted that all 18 security configuration profiles did not meet industry best practices for recommended mobile device security settings (Finding 3).		X	Agrees

Audit Objective	Audit Conclusion
Objective 3: To assess the effectiveness of DTMB's efforts to ensure that only authorized devices access the State's IT resources.	Moderately effective

Finding Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB had not implemented sufficient controls to ensure that only authorized mobile devices access the State's IT resources, thereby increasing the risk to confidential and sensitive data (Finding 4).		X	Agrees

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

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

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

Doug A. Ringler, CPA, CIA
Auditor General

January 22, 2015

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

Dear Mr. Behen:

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

This report contains our report summary; a description; our audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of abbreviations and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's response at the end of our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

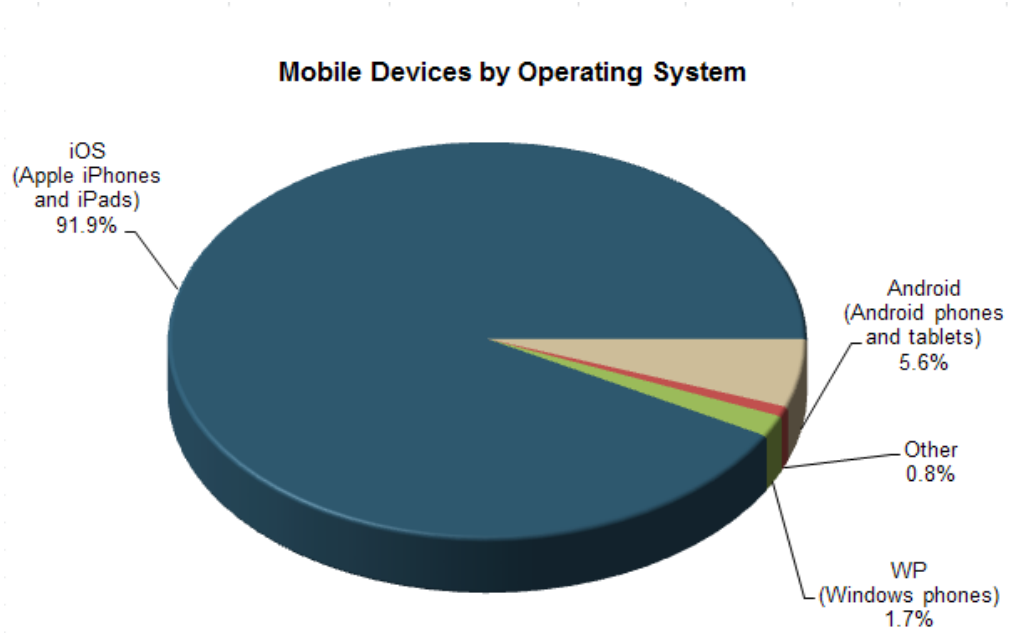
TABLE OF CONTENTS

DATA SECURITY USING MOBILE DEVICES
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Mobile Devices

Mobile devices (also known as smart devices), including smartphones and tablet computers with iOS and Android operating systems, have computing power equivalent to traditional personal computers but with the convenience of portability. Although mobile devices have increased productivity and enhanced customer service, they also have increased the potential for unauthorized access to an organization's information technology* (IT) resources.

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, file servers, and information systems. Between June 1, 2014 and July 1, 2014, over 11,500 mobile devices connected to the State's IT resources. The following chart summarizes the percentage of mobile devices, by operating system, that connected to the State's IT resources:



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

Mobile Device Management (MDM) System

The Department of Technology, Management, and Budget (DTMB) uses an MDM System to manage the State employees' use of mobile devices. An MDM System allows for the central configuration and management of network enabled mobile devices. DTMB implemented an MDM System in January 2013. The State's MDM System can manage the three most popular mobile device platforms (iOS, Android, and Windows phone) and configure and enforce security* features for enrolled mobile devices that connect to the State's IT resources using ActiveSync*.

Office Automation Services (OAS), Smart Device Support Team (SDST)

DTMB's OAS is responsible for simplifying, standardizing, and supporting the State's IT resources. SDST functions as the support center for State employees needing assistance with mobile devices. In addition, SDST is responsible for configuring and managing mobile devices using the State's MDM System.

Cybersecurity and Infrastructure Protection (CIP)

DTMB's CIP is responsible for providing oversight of risk management and security issues associated with the State's assets, systems, and networks. In addition, CIP is responsible for aiding in the development and implementation of a comprehensive security strategy for all of the State's IT resources, including mobile devices.

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

Audit Objectives

Our performance audit* of Data Security Using Mobile Devices, Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to establish a governance structure and provide guidance regarding mobile device security.
2. To assess the effectiveness of DTMB's efforts to design, implement, and enforce the secure configuration of mobile devices.
3. To assess the effectiveness of DTMB's efforts to ensure that only authorized devices access the State's information technology (IT) resources.

Audit Scope

Our audit scope was to examine the governance structure and controls over security of mobile devices that access the State's IT resources. We limited our review to devices that accessed the State's IT resources using mobile operating systems, which included iOS, Android, and Windows phone devices. Our review did not include intel-chip based products, such as laptop computers, netbooks, hybrid laptops, or Windows surface tablets. In addition, we did not review portable storage devices that do not have an operating system, such as USB flash drives or portable hard drives. 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 procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2012 through October 31, 2014.

Audit Methodology

We conducted a preliminary survey of controls over mobile devices, including configuration controls, access controls*, and governance structure. We interviewed

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

various officials from DTMB and reviewed data from the State's Mobile Device Management (MDM) System to gain an understanding of the mobile device environment. Also, we conducted a survey of mobile device users within the State of Michigan to ascertain how mobile devices were being used by State employees. We used the results of our preliminary survey to determine the extent of our detailed analysis and testing.

To accomplish our first audit objective, we:

- Identified DTMB policies, standards, and procedures related to the security of mobile devices.
- Compared DTMB's mobile device policies, standards, and procedures to industry best practices, including the National Institute of Standards and Technology* (NIST) and Control Objectives for Information and Related Technology* (COBIT).
- Reviewed DTMB's governance structure over the security of mobile devices.

To accomplish our second audit objective, we:

- Reviewed data from the State's MDM System.
- Compared the State's MDM System mobile device configuration policies to vendor supplied recommended settings as well as State IT policies and standards.
- Reviewed mobile device configurations for compliance with MDM configuration profiles.
- Reviewed users with access to the State's MDM System's configuration settings and verified that those users had an appropriate business need to access the State's MDM System.

To accomplish our third audit objective, we:

- Obtained inventories of mobile devices from the 18 executive branch departments.

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

- Compared the inventories of mobile devices to information within the State's MDM System and identified devices within the MDM System that did not appear in State department inventories.
- Obtained an understanding of how DTMB uses ActiveSync to identify mobile devices accessing the State's IT resources.

We based our audit conclusions on our audit efforts as described in the preceding paragraphs and the resulting material condition* and reportable conditions* noted in the comments, findings, recommendations, and agency preliminary responses section. The material condition is more severe than the reportable conditions and could impair management's ability to operate effectively or could adversely affect the judgment of an interested person concerning the effectiveness of the security of mobile devices. The reportable conditions are less severe than the material condition but represent deficiencies in internal control*.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve the operations of State government. Consequently, we prepare our performance audit reports on an exception basis.

Agency Responses

Our audit report contains 4 findings and 4 corresponding recommendations. DTMB's preliminary response indicates that it agrees with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

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

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO ESTABLISH A GOVERNANCE STRUCTURE AND PROVIDE GUIDANCE REGARDING MOBILE DEVICE SECURITY

COMMENT

Audit Objective: To assess the effectiveness of the Department of Technology, Management, and Budget's (DTMB's) efforts to establish a governance structure and provide guidance regarding mobile device security.

Audit Conclusion: Moderately effective.

Factors leading to this conclusion included the:

- Development of a mobile computing strategy by a third party consulting firm.
- Lack of an enforcement role within the governance structure.
- Implementation of the State's Mobile Device Management (MDM) System.
- Establishment of centralized mobile device support.
- Reportable condition related to a governance structure over mobile device security.

FINDING

1. Governance Structure

   DTMB had not fully established an effective governance structure over the security of mobile devices. As a result, DTMB could not ensure that mobile devices were appropriately managed and secured.

   According to Control Objectives for Information and Related Technology (COBIT), an information security governance structure is established through policy development. A governance structure is necessary for identifying roles and responsibilities related to management and oversight of mobile device security. As the State's central management and control agency, DTMB is responsible for developing and implementing processes to replicate and enforce information technology (IT) best practices and standards throughout the executive branch of State government.

Our review of DTMB's mobile device security governance structure disclosed:

a. DTMB had not established, assigned, or communicated the roles, responsibilities, and expectations for monitoring mobile devices and enforcing the secure configuration of mobile devices. As a result, no one was centrally performing the responsibilities associated with mobile device security.

   According to COBIT, managing mobile device security includes roles and responsibilities, such as defining a mobile security strategy, developing a mobile device security standard, identifying end-user responsibilities for mobile device security, and monitoring the security of mobile devices.

b. DTMB had not established or updated the State's IT policies, standards, and procedures to sufficiently address the use and security of mobile devices. Lack of established and updated policies, standards, and procedures providing clear guidance on the security of mobile devices may result in data being lost or disclosed to unauthorized individuals.

   The National Institute of Standards and Technology (NIST) Special Publication 800-124 states that an organization should:

   - Allow devices to only install approved applications from authorized "app stores*."
   - Limit the types of mobile devices that may be used for accessing the State's IT resources based on the risk presented by each type of device.
   - Remove sensitive data from mobile devices in a secure manner prior to the devices being disposed or reassigned.

   Our review disclosed:

   (1) DTMB had not established an application management policy for mobile devices.

   (2) DTMB had not updated Technical Standard 1345.00.07 to identify mobile devices approved for use in the State's IT environment.

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

(3) DTMB had not updated Technical Standard 1340.00.13 to identify acceptable methods for securely removing data from mobile devices prior to disposal or reassignment.

DTMB informed us that a fully established governance structure had not been implemented because a governance board was not established. DTMB indicated that a governance board will be created to establish or update, as necessary, the State's existing IT policies, standards, and procedures to sufficiently address the use and security of mobile devices.

RECOMMENDATION

We recommend that DTMB fully establish an effective governance structure over the security of mobile devices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will establish an effective governance structure over mobile devices. DTMB will establish a governance board consisting of members of the Customer Service Partnership Security Sub-committee. In addition, DTMB will develop a mobile device security standard, update applicable technical standards, and identify end-user responsibilities for mobile device security.

EFFECTIVENESS OF EFFORTS TO DESIGN, IMPLEMENT, AND ENFORCE THE SECURE CONFIGURATION OF MOBILE DEVICES

COMMENT

Audit Objective: To assess the effectiveness of DTMB's efforts to design, implement, and enforce the secure configuration of mobile devices.

Audit Conclusion: Not effective.

Factors leading to this conclusion included the:

- Capability to access and store sensitive data on mobile devices.
- Increased exposure to threats* and risk of data compromise from the mobility and portability of the devices.
- Number of mobile devices within State government that are unmanaged.
- Material condition related to the lack of enforcement of mobile device security configuration profiles.
- Reportable condition related to the establishment of security configurations for mobile devices.

FINDING

2. Security Configuration Enforcement

DTMB did not enforce security configuration profiles within the State's MDM System to ensure that controls over patch management, access, encryption, and virus protection were implemented. Without enforcement, confidential and sensitive data was at a greater risk of being compromised.

According to NIST Special Publication 800-124, effective implementation of mobile device security requires that administrators have the ability to manage all components of the security solution.

We reviewed data within the State's MDM System regarding the status of mobile devices that accessed the State's IT resources via ActiveSync between June 1, 2014 and July 1, 2014. Our review disclosed:

a. DTMB did not enforce the enrollment of all mobile devices within the State's MDM System. We noted that 1,940 (16.8%) of the 11,525 mobile devices

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

were not managed by the State's MDM System. The following table summarizes these mobile devices by executive branch department:

Executive Branch Department	Number of Mobile Devices			Percent of Mobile Devices Not Managed by the State's MDM System
	Total	Managed by the State's MDM System	Not Managed by the State's MDM System	
Human Services	4,261	4,185	76	1.8%
Transportation	1,568	1,542	26	1.7%
State Police	1,298	1	1,297	99.9%
Technology, Management, and Budget	1,207	1,002	205	17.0%
Licensing and Regulatory Affairs	614	588	26	4.2%
Corrections	542	451	91	16.8%
Treasury	318	293	25	7.9%
Education	306	280	26	8.5%
Community Health	284	272	12	4.2%
Agriculture and Rural Development	280	219	61	21.8%
Natural Resources	277	253	24	8.7%
Environmental Quality	238	228	10	4.2%
Attorney General	88	49	39	44.3%
Insurance and Financial Services	66	61	5	7.6%
State	65	57	8	12.3%
Military and Veterans Affairs	53	48	5	9.4%
Civil Service Commission	38	34	4	10.5%
Civil Rights	22	22	0	0.0%
Total	11,525	9,585	1,940	16.8%

b. DTMB did not enforce compliance with the security configuration profiles established within the State's MDM System. We noted that 270 (2.8%) of the 9,585 mobile devices that were managed in the MDM System were not in compliance with the MDM System's configuration settings protecting against threats, such as passcode rule violations and jailbreaking* or rooting* a mobile device.

c. DTMB did not follow up on instances in which data within the State's MDM System did not contain information on the compliance status of security configuration profiles for managed mobile devices. We noted that for

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

2,652 (27.7%) of the 9,585 enrolled mobile devices, the State's MDM System did not contain enough information for DTMB to determine the full compliance status of the mobile device.

DTMB informed us that it had not enforced security configuration profiles because it had not established a governance board. It expects a governance board to set security policy and enforcement response actions.

RECOMMENDATION

We recommend that DTMB enforce security configuration profiles within the State's MDM System.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will enforce security configuration profiles within the State's MDM System. DTMB will ensure that required data is in the MDM System to determine full compliance with security configurations. DTMB will enforce enrollment in the MDM System for all connected devices and enforce compliance with the configuration profiles. In addition, DTMB will develop a process to review MDM System data and remediate issues as necessary.

FINDING

3. Security Configuration Management*

DTMB had not fully established effective security configurations for mobile devices. As a result, DTMB could not ensure that data stored or accessed by mobile devices was protected from unauthorized loss or disclosure.

DTMB Technical Standard 1340.00.03 requires the secure establishment, maintenance, and administration of all IT resources. To achieve a secure configuration, the Standard requires that controls be established to protect information and resources from unauthorized access.

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

DTMB created 18 security configuration profiles that it may apply to mobile devices enrolled within the State's MDM System. We reviewed these profiles and selected security settings for active mobile devices that accessed the State's IT resources between June 1, 2014 and July 1, 2014. We identified potentially vulnerable configurations, according to vendor supplied recommended settings, on all 18 profiles. In addition, none of the 18 profiles consistently incorporated established DTMB technical standards. Because of the confidential nature of security configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB.

DTMB informed us that security configurations were not fully established because DTMB had not established a governance board. It expects a governance board to set security policy and enforcement response actions.

RECOMMENDATION

We recommend that DTMB fully establish effective security configurations for mobile devices.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will establish effective security configurations for mobile devices that access the State's IT resources. DTMB will establish and implement security configuration profiles within the State's MDM System, based on NIST recommendations.

EFFECTIVENESS OF EFFORTS TO ENSURE THAT ONLY AUTHORIZED DEVICES ACCESS THE STATE'S IT RESOURCES

COMMENT

Audit Objective: To assess the effectiveness of DTMB's efforts to ensure that only authorized devices access the State's IT resources.

Audit Conclusion: Moderately effective.

Factors leading to this conclusion included:

- The inconsistent and decentralized approach to managing mobile device inventory.
- DTMB's ability to identify all devices accessing the State's IT resources via ActiveSync.
- The reportable condition related to controls to ensure that only authorized mobile devices access the State's IT resources.

FINDING

4. Mobile Device Authorization

DTMB had not implemented sufficient controls to ensure that only authorized mobile devices access the State's IT resources. As a result, DTMB could not ensure that all mobile devices accessing the State's IT resources met the necessary security requirements and had authorized access.

According to COBIT DSS05.02, Manage Network and Connectivity Security, organizations should allow only authorized devices to access business information and the enterprise network.

We reviewed DTMB's process for allowing mobile devices to access the State's IT resources. Also, we compared mobile devices accessing the State's IT resources identified within the State's MDM System with mobile device inventories maintained by the 18 executive branch departments to identify devices that did not appear in those inventories. Our review disclosed:

a. DTMB did not manage mobile device access to the State's IT resources at the device level and instead controlled an individual's access using ActiveSync. At the time of our audit, users with State of Michigan credentials could use any mobile device they possessed to access the State's IT resources via ActiveSync without the mobile device having been authorized. Because of the sensitive nature of security controls, we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB. Controlling access at the mobile device level in addition to the user level would allow DTMB to ensure that all mobile devices accessing the State's IT resources meet the security requirements.

DTMB Technical Standard 1335.00.03 requires information systems to uniquely identify and authenticate devices before establishing a connection to the State's network.

b. DTMB did not maintain a central inventory of mobile devices authorized to access the State's IT resources.

According to NIST Special Publication 800-124, keeping an active inventory of each mobile device, its user, and its applications is an important process for centrally managing mobile device security. Also, the SANS Institute's* Critical Security Control 1 states that organizations should inventory, track, and regulate all hardware devices on a network so that only authorized devices are given access and unauthorized and unmanaged devices are prevented from gaining access.

Between June 1, 2014 and July 1, 2014, we identified 297 instances in which a mobile device appeared within the State's MDM System as having accessed the State's IT resources via ActiveSync but did not appear in any of the inventory listings maintained by the 18 executive branch departments. Because a centralized inventory of authorized mobile devices was not developed and access was controlled at the user level, as discussed in part a. of this finding, DTMB was unable to determine if the 297 instances were from unauthorized employee-owned personal devices that accessed the State's IT resources. A centralized inventory of all mobile devices authorized to access the State's IT resources would improve DTMB's ability to control access at the mobile device level to ensure that all connected devices are authorized.

DTMB informed us that mandatory loading of the State's MDM System software on mobile devices had not been required pending implementation of DTMB Technical Standard 1340.00.12. DTMB also informed us that it was piloting the Standard and associated procedures and planned to implement them on December 1, 2014.

RECOMMENDATION

We recommend that DTMB implement sufficient controls to ensure that only authorized mobile devices access the State's IT resources.

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will implement controls to ensure that only authorized mobile devices access the State's IT resources. DTMB will develop specific guidance for agencies to implement effective inventory controls. In addition, DTMB will establish and maintain a central inventory of mobile devices (personal and State-owned) that are authorized to access the State's IT resources and establish a periodic review process for mobile devices accessing the State's IT resources.

GLOSSARY

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.
ActiveSync	A client protocol that lets the user synchronize a mobile device with the user's Exchange mailbox.
app store	An on-line portal through which software programs are made available for purchase and download for mobile devices.
CIP	Cybersecurity and Infrastructure Protection.
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.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
information technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
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.
jailbreaking	The process of removing restrictions on iOS mobile devices to provide privilege root access to the iOS file system and manager. This provides greater flexibility and control over the device but also bypasses important security features, which may allow the introduction of vulnerabilities.
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.
MDM	Mobile Device Management.
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.
OAS	Office of Automation Services.
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 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.
rooting	The process of removing restrictions on Android mobile devices to provide privilege root access to the operating system and manager. This provides greater flexibility and control over the device but also bypasses important security features, which may allow the introduction of vulnerabilities.
SANS Institute	A research and education organization that develops, maintains, and makes available at no cost research documents about various aspects of information security. The SANS Institute also offers computer security training and certification.
SDST	Smart Device Support Team.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
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

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL