



Performance Audit

Report Number:
071-0555-14

Data Security Using Mobile Devices

Department of Technology, Management, and Budget

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 (<u>Finding 3</u>).		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 (<u>Finding 4</u>).		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