



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

APR 5 2013

MEMORANDUM FOR ARMY CHIEF INFORMATION OFFICER
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: DoD Inspector General Report No. DODIG-2013-060, "Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices," March 26, 2013

We are revising the management comments section in the subject report to address updated Army information identified after publishing the original report. We removed the original report from our Web site pending review of the updated information. The revised report, which incorporates the updated information, is posted in electronic version on our Web site at <http://www.dodig.mil/Audit/reports/index.html>.

We included the revised comments the Director, Army CIO/G-6, provided on March 26, 2013, in response to the recommendations. The revisions are minor and do not affect the overall findings, conclusions, or recommendations presented in the original report.

If you have any questions on the revisions, please contact me at (703) 604-8866.

A handwritten signature in blue ink, reading "Alice F. Carey", is positioned above the typed name.

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

Army Chief Information Officer Comments



Office, Chief Information Officer / G-6

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

MAR 26 2013

SAIS-CBB

MEMORANDUM FOR PROGRAM DIRECTOR READINESS, OPERATIONS AND
SUPPORT, DEPARTMENT OF DEFENSE INSPECTOR GENERAL, 4800 MARK
CENTER DRIVE, ALEXANDRIA, VIRGINIA 22350-1500

SUBJECT: CIO/G-6 Cybersecurity Directorate Response to Follow-up Questions on
Department of Defense (DOD) Inspector General Agency Draft Report Improvements
Needed with Tracking and Configuring Army Commercial Mobile Devices

1. References: Department of Defense Office of Inspector General Draft Report
Improvements Needed with Tracking and Configuring Army Commercial Mobile Devices
(Project No. D2012-D000LC-0147.000) and follow-up questions from [REDACTED]
2. The CIO/G-6 concurs, with comments, with the draft report Improvements Needed
with Tracking and Configuring Army Commercial Mobile Devices. In many cases, the
Army has already implemented improvements.
3. The point of contact for this action is [REDACTED] at: [REDACTED] or
email: [REDACTED]

Encl

STUART M. DYER
Major General, GS
Director, Army CIO/G-6 Cybersecurity Directorate
Army Senior Information Assurance Officer

UNCLASSIFIED

ENCLOSURE: CIO/G-6 Cybersecurity Directorate Second Response to Department of Defense Office of Inspector General Draft Report Improvements Needed with Tracking and Configuring Army Commercial Mobile Devices (Project No. D2012-D000LC-0147.000)

Objective: To determine whether the Department of the Army had an effective cybersecurity program that identified and mitigated risks surrounding commercial mobile devices (CMDs) and removable media. Specifically, at the sites visited, we verified whether Army officials appropriately tracked, configured, and sanitized CMDs. Additionally, we determined whether the Army used authorized removable media on its network.

Finding: The Army Chief Information Officer (CIO) did not implement an effective Cybersecurity program for CMDs. Specifically, the Army CIO did not appropriately track CMDs and was unaware of more than 14,000 CMDs used throughout the Army.

Recommendation 1

The Chief Information Officer, Department of the Army, develop clear and comprehensive policy to include requirements for reporting and tracking all commercial mobile devices (CMD) purchased under pilot and non-pilot programs.

Chief Information Officer/G-6 Response:

Concur that the Army develop clear and comprehensive policy to include requirements for pilot approval of CMDs.

Currently the Army has numerous approved mobile pilots and is also a participant in the DoD/DISA Mobile pilot. The Army CIO, LTG Lawrence signed the memorandum titled "U.S. Army Guidance on Piloting of Commercial Mobile Devices, dated Nov 3, 2011. This memorandum directs Army organizations to register each mobile pilot. The Army Cybersecurity Directorate maintains a SharePoint Portal where an Army organization must register a mobile pilot and provide project artifacts. An Army Senior Leader, who has the authority to accept risk and to make decision for the designated organization, provides the artifacts in the form of a declaration or through an on line survey. The registration process ensures that sensitive information (FOUO) and Personal Identifiable Information (PII) is not allowed and the platform cannot connect to the Army email system. On 3 April 2012 the Secretary of the Army signed a memorandum titled "Mobile Computing Devices" and stated no unauthorized CMDs will be connected to the NIPRnet or used to conduct official business.

This guidance and direction was communicated to all the Army Information Assurance Program Managers (IAPMs) across the Army as well as during the Mobile Electronic Working Groups. In summary, no CMDs are currently allowed for Army use outside of authorized pilots and policy and guidance has been promulgated.

A Headquarters Department of Army (HQDA) staff element that approves an Army pilot would not maintain property accountability for any equipment that is purchased to support that pilot. The organization that purchases the equipment is responsible for maintaining accountability IAW Army property accountability regulations and procedures.

UNCLASSIFIED

UNCLASSIFIED

ENCLOSURE: CIO/G-6 Cybersecurity Directorate Second Response to Department of Defense Office of Inspector General Draft Report Improvements Needed with Tracking and Configuring Army Commercial Mobile Devices (Project No. D2012-D000LC-0147.000)

It is also important to note that the number of devices that an organization purchases to support a pilot is not important. What is important is that the devices are used IAW the policy and guidelines that were approved for the pilot.

Recommendation 2

The Chief Information Officer, Department of the Army, should designate commercial mobile devices as information systems and extend existing information assurance requirements to the use of commercial mobile devices.

Chief Information Officer/G-6 Response:

Concur that the Army should extend existing information assurance requirements to the use of commercial mobile devices, but the Army will not establish CMDs as a separate/stand alone system. A CMD is an extension of the existing Information System and does not require a separate designation; it provides an interface to an existing system or environment and will fall under the Control of the Host system. In order to further support the position of not considering a CMD an information system, the Army, along with DoD and DISA, are working to establish the ability to manage Mobile Devices. Mobile devices will be managed utilizing a Mobile Device Management (MDM) system in concert with a Mobile Application Store (MAS). End state will be the DoD Enterprise ability to observe every managed Mobile device, as well as every application operating on a DoD-managed Commercial Mobile Device. This action is in development, projected to be in place by the end FY14. This capability is addressed in the DoD memorandum that the DoD CIO signed titled "DoD Commercial Mobile Implementation Plan" dated February 2013.

Recommendation 3

The Chief Information Officer, Department of the Army, develop a process to verify that users of commercial mobile devices are following Army and DoD information assurance policies and implementing the appropriate security controls to protect commercial mobile devices.

Chief Information Officer/G-6 Response:

Concur that the Army leverage a process to verify that users of CMDs follow Army and DoD information assurance policies and implement the appropriate security controls to protect CMDs.

The Army has already transitioned over 1 million users to the DoD/DISA email enterprise unclassified email system. DISA has become the Army's service provider. As DISA establishes the MDM and MAS architecture, Army mobile devices will become managed mobile devices. The governance and oversight will be established as a DISA service. This capability will include visibility, oversight of proper configuration, and management

UNCLASSIFIED

UNCLASSIFIED

ENCLOSURE: CIO/G-6 Cybersecurity Directorate Second Response to Department of Defense Office of Inspector General Draft Report Improvements Needed with Tracking and Configuring Army Commercial Mobile Devices (Project No. D2012-D000LC-0147.000)

of all devices. Additionally, the capability to wipe or remove a device from the environment and the ability to monitor usage of a mobile device with respect to applications utilized, web sites visited, and data viewed, saved or modified will also be available. The policy is in place to require the Army to utilize the MDM and MAS. This action is in development and planned to be in place by the end of FY14. The Request for Proposal (RFP) for the MDM and MAS has closed and the determination of the award is projected for April 2013. The build out and implementation of the awarded solution is projected to achieve Initial Operating Capability (IOC) by October 2013 with Full Operating Capability (FOC) to follow before the end of FY14.

DoD has issued over 30 policies memos, Security Requirements Guides (SRG), and Security Technical Implementation Guides (STIG) that apply to mobile technology. Detailed information on DoD mobile security policies can be found at <http://iase.disa.mil/stigs/a-z.html>. As a component of DoD, the Army is required to comply with these regulations. The DoD Instruction 8100.04 "DoD Unified Capabilities", dated 9 DEC 2010, states that all devices that provide unified communications (including CMDs) must have appropriate technical and security documents in place. The instruction specifically requires the use SRGs and STIGs to prescribe the requirements and implementation details for the testing, certification, acquisition, and operation of devices that provide unified communications. IA testing shall be conducted pursuant to these guidelines prior to operation of products. Subsequently, DISA produced the Mobile Device Management (MDM) SRG, the Wireless Smartphone SRG, the Mobile OS SRG, as well as STIGs for Apple iOS, Android OS, and Blackberry OS. Seeing that the Army utilizes DISA as the enterprise solution provider for CMDs, we are compelled to comply with the MDM SRG, Mobile OS SRG/STIGs, and all future policies related to mobile technology.

UNCLASSIFIED