Report No. DODIG-2013-060 March 26, 2013

Inspector General
United States Department of Defense

Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
26 MAR 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Inspector General of the Department of Defense,400 Army Navy Drive,Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**26**	

Additional Copies

To obtain additional copies of this report, visit the Department of Defense Inspector General website at http://www.dodig.mil/pubs/index.cfm, or contact the Secondary Reports Distribution Unit at auditnet@dodig.mil.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing at auditnet@dodig.mil or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

Acronyms and Abbreviations

CIO	Chief Information Officer
CMD	Commercial Mobile Device
ERDC	Engineer Research and Development Center
IA	Information Assurance
MDM	Mobile Device Management
MICA	Mobile Information Collection Application
PED	Portable Electronic Device
USACE	United States Army Corps of Engineers
USMA	United States Military Academy

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

MAR 26 2013

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

SUBJECT: Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices (Report No. DODIG-2013-060)

We are providing this report for review and comment. The Army did not implement an effective cybersecurity program for commercial mobiles devices. If devices remain unsecure, malicious activities could disrupt Army networks and compromise sensitive DoD information. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We received comments from the Director, Army Chief Information Officer Cybersecurity Directorate on behalf of the Chief Information Officer, Department of the Army. The Director's comments on Recommendations 1 and 2 were nonresponsive. Therefore, we request additional comments from the Chief Information Officer, Department of the Army, on these recommendations by April 25, 2013. We considered the Director's comments on Recommendation 3 responsive.

Please provide comments that conform to the requirements of DoD Directive 7650.3. If possible, send a portable document file (.pdf) containing your comments to audros@dodig.mil. Copies of management comments must have the actual signature of the authorizing official. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8866 (DSN 664-8866).

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

Results in Brief: Improvements Needed With Tracking and Configuring Army Commercial Mobile Devices

What We Did

Our objective was 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.

What We Found

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. Additionally, at the sites visited, the Army CIO did not:

- ensure that Commands configured CMDs to protect stored information. The CIOs at United States Military Academy (USMA) and United States Army Corps of Engineers (USACE) Engineer Research and Development Center (ERDC) did not use a mobile device management application to configure all CMDs to protect stored information.
- require CMDs to be properly sanitized. CIOs at USMA and USACE ERDC did not have the capability to remotely wipe data stored on CMDs that were transferred, lost, stolen, or damaged.
- control CMDs used as removable media. The CIOs at USMA and USACE ERDC allowed users to store sensitive data on CMDs that acted as removable media.
- require training and use agreements specific to CMDs. The CIOs at USMA and USACE ERDC did not train CMD users and require users to sign user agreements.

These actions occurred because the Army CIO did not develop clear and comprehensive policy for CMDs purchased under pilot and non-pilot programs. In addition, the Army CIO inappropriately concluded that CMDs were not connecting to Army networks and storing sensitive information. As a result, critical information assurance controls were not appropriately applied, which left the Army networks more vulnerable to cybersecurity attacks and leakage of sensitive data.

What We Recommend

The Army CIO should develop clear and comprehensive policy to include requirements for reporting and tracking all CMDs. In addition, the Army CIO should extend existing information assurance requirements to the use of all CMDs.

Management Comments and Our Response

The Director, Army CIO Cybersecurity Directorate provided comments on behalf of the Army CIO, and agreed with the report recommendations, but the comments on Recommendations 1 and 2 were nonresponsive. We request comments in response to the final report by April 25, 2013. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Chief Information Officer, Department of the Army	1, 2	3

Please provide comments by April 25, 2013.

Table of Contents

Introduction

Objectives

Our objective was to determine whether the Department of the Army had an effective cybersecurity program that identified and mitigated risks surrounding portable electronic devices (PEDs) and removable media. Specifically, at the sites visited, we verified whether Army officials appropriately tracked, configured, and sanitized PEDs. Additionally, we determined whether the Army used authorized removable media on its network. For a discussion on scope and methodology, see the Appendix.

Considering the broad definition of PEDs [1], we limited our review to commercial mobile devices (CMDs) running on the Apple iOS, Android, and Windows mobile operating systems. In addition, we excluded BlackBerry devices because the DoD OIG issued a report on September 25, 2009, "Controls Over Information Contained in BlackBerry Devices Used Within DoD" (DoD IG Report No. D-2009-111). Furthermore, our review focused on the use of CMDs as removable media and the removable media within the CMDs.

Adopting New Technologies

With the rapid changes in information technology, the Army decided to adopt newer technologies, starting with incorporating CMDs into daily activities. As the Army adopted this newer technology, it began testing CMDs in the field and in administrative offices. In 2009, the Army Vice Chief of Staff directed the Army Chief Information Officer (CIO) to begin procuring inexpensive systems such as Apple iPhone and Google Android CMDs instead of the traditional procurement of dedicated software and hardware. DoD explored options to procure devices, such as Apple and Android products.

DoD Mobile Device Strategy

In June 2012, the DoD CIO released the DoD Mobile Device Strategy to identify the vision and goals for using the full potential of mobile devices. The strategy focused on the following areas of improvement critical to mobility.

- wireless infrastructure to support the secure access and sharing of information via voice, video, or data by mobile devices;
- policies, processes, and standards to support secure mobile device usage, device-to-device interoperability, and consistent device lifecycle management;
- processes and tools to enable consistent development, testing, and distribution of DoD-approved mobile applications for faster deployment to the user; and

[1] Army Regulation 25-2 defines a PED as a portable device with or without the capability of wireless or local area network connectivity. PEDs include cell phones, tablets, pagers, personal digital assistants, laptops, memory sticks, thumb drives, and two-way radios. In addition, the Army CIO further states CMDs are tablets and smartphones that have a unique combination of computing power, mobile applications, and access to network data, which sets CMDs apart from other PEDs.

- policies, processes, and mechanisms for appropriately Web-enabling critical DoD information technology systems and functions for mobile devices.

Army Chief Information Officer Responsibilities

The Army CIO is responsible for supervising Army information technology functions and advising the Chief of Staff of the Army on network, communications, and signal operations. In addition, the Army CIO manages the Army cybersecurity program, which includes analyzing and improving business processes, and managing information resources, acquisitions, and training. According to Army Regulation 25-1, "Army Knowledge Management and Information Technology," December 4, 2008, the Army CIO must provide oversight of the Army information assurance program. In 2010, the Army CIO released guidance for the Army on piloting and integrating new mobile device technologies, requiring any Army command or organization to identify the mobile device activities to the Army CIO. In 2011, the Army CIO issued additional guidance requiring all Army pilots using CMDs to obtain pilot authorization so that the Army CIO could track and share lessons learned and prevent duplication of effort.

Risks of CMDs

Both the DoD CIO and the Army CIO recognized the risk of emerging CMD technologies on DoD information. Applications installed on devices may contain malware or spyware, or may perform unexpected functions such as tracking user actions or sending private information to outsiders. Additionally, hackers can access features on devices such as the Bluetooth or Wi-Fi radios connected to devices without the user's knowledge. Most CMDs, as purchased, do not come equipped with the security controls and other necessary security features required by DoD, presenting an undue risk to the enterprise.

CMDs Used by Army Activities Visited

We conducted a datacall requesting a list of all smartphones (excluding BlackBerry devices) and tablets that the Army procured from October 1, 2010, through May 31, 2012. We received a list of more than 14,000 CMDs used throughout the Army. As a result of the responses, we visited two sites to verify whether the CMDs in use were appropriately tracked, configured, and sanitized, and followed policy for using CMDs as removable media. Specifically, we visited the United States Military Academy (USMA) at West Point, New York, and the United States Army Corps of Engineers (USACE), Engineer Research and Development Center (ERDC) at Vicksburg, Mississippi. USMA reported 276 CMDs, and USACE ERDC reported 276 CMDs, totaling 552 CMDs. USACE ERDC reported an additional 290 CMDs during the site visit, which increased the number of devices at the two locations to 842. The number of CMDs listed in the table represents the number that each site reported to the DoD Office of Inspector General (OIG) and does not reflect the total number of devices each site actually used. The following table shows how each location used the devices, the total number reported, and total estimated cost of those devices.

Table. CMDs Reported by USMA and USACE ERDC

Site	Device Usage	Number of Devices	Total Estimated Cost
USMA	Research Devices	276	$242,444*
USACE ERDC	Pilot Devices	276	122,400
	Non-Pilot Devices	290	120,950
Total		**842**	**$485,794**

* This represents cost for 266 devices. USMA was unable to provide cost for 10 devices.

The following outlines the number of devices tested at each site location. At USMA, we selected 72 CMDs to test; however, we tested only 48 CMDs because 24 of the 72 CMDs were in the possession of faculty members and cadets who were not on site. In addition, we selected 71 devices at USACE ERDC. During the site visit, the Program Manager informed the team that USACE ERDC had an additional 290 non-pilot devices, which increased the number of devices to 566 CMDs. As a result, we selected an additional 72 CMDs to test, for a total of 143 CMDs at USACE ERDC. However, we tested only 133 CMDs (62 non-pilot general research CMDs and 71 pilot CMDs) because 10 CMDs were in the possession of personnel who were unavailable.

CMDs Used by United States Military Academy

USMA trains cadets to become officers in the United States Army. USMA originally acquired CMDs for use in a pilot program to assess the usability of the devices in support of the academic program. The assessment provided USMA an opportunity to discover what enhancements are possible for using CMDs to educate cadets. USMA also procured CMDs for other research purposes, such as a military history e-book, that leverages the capabilities of mobile devices. Cadets and faculty also examined mobile device security and application development using CMDs.

CMDs Used by United States Army Corps of Engineers, Engineer Research and Development Center

USACE ERDC acquired CMDs for both pilot and non-pilot programs. USACE ERDC has two pilot programs: Mobile Information Collection Application (MICA) and Blue Roof. In addition, USACE ERDC labs use CMDs for general research.

USACE ERDC Mobile Information Collection Application Pilot Program

The MICA pilot program uses CMDs to replace the manual field data collection process during a natural disaster. Using the device's built-in capabilities, personnel could take a picture, automatically capture the latitude and longitude, add notes, and instantly upload the data to the server for analysis if Internet access were available. In areas with no

access available, the device stores the data until the individual returns to a location with access. These capabilities allow decision makers to have immediate feedback on flood conditions.

USACE Blue Roof Pilot Program

Working under the authority of the Federal Emergency Management Agency, USACE contractors can prevent additional damage to homes after a hurricane or other disaster by installing blue plastic sheeting as part of the Operation Blue Roof program. CMDs replace paper forms by capturing the information digitally in the beginning. Homeowners use the CMD to request assistance and to provide the authorization for USACE personnel to enter the property, but the system automatically disqualifies homeowners who live outside an affected area and assigns an inspector for homes that qualify. Inspectors use the CMD to enter photos and notes, as well as the quantity of materials needed to repair the home.

General Research Programs

USACE ERDC also uses CMDs as part of general research programs. Research projects at USACE ERDC varied from application development to e-readers for scholarly journals. Additionally, USACE ERDC employees used these devices for personal use.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses for Army. The Army CIO did not implement an effective cybersecurity program for CMDs because they did not develop clear and comprehensive policy related to all CMDs. In addition, the Army CIO inappropriately concluded that CMDs were not connecting to Army networks and storing sensitive information; and, therefore, did not extend current IA requirements to the use of CMDs. We will provide a copy of the report to the senior official responsible for internal controls in the Department of the Army.

Finding. Cybersecurity Program for CMDs Needs Improvement

The Army CIO did not implement an effective cybersecurity program applicable to CMDs. Specifically, the Army CIO did not appropriately track more than 14,000 CMDs purchased as part of pilot and non-pilot programs[2]. In addition, at the two sites visited, the Army CIO did not:

- ensure that Commands configured CMDs adequately to secure data stored on the device,
- require all CMDs to be sanitized before transfer or loss,
- control CMDs used as removable media, and
- require training and user agreements specific to CMDs.

This occurred because the Army CIO did not develop clear and comprehensive policy for CMDs purchased under pilot and non-pilot programs. In addition, the Army CIO inappropriately concluded that CMDs were not connecting to Army networks and storing sensitive information; and, therefore, did not extend current IA requirements to the use of CMDs. Without an effective cybersecurity program specific to CMDs, critical IA controls necessary to safeguard the devices were not applied, and the Army increased its risk of cybersecurity attacks and leakage of sensitive data.

Guidance on the Use of CMDs

DoD CIO Memorandum, "Use of Commercial Mobile Devices in the Department of Defense," April 6, 2011, provides security objectives for CMDs that outline current challenges and potential mitigation activities. The memorandum requires Component CIOs to review security requirements for using CMDs and to implement controls to address the following:

- using an enterprise management system to manage and control CMDs,
- encrypting and sanitizing sensitive DoD information stored on CMDs,
- granting access to CMDs through DoD identification and authentication requirements,
- using private key infrastructure credentials to send and receive e-mail messages,
- installing designated approving authority-approved software and applications, and
- training users on CMDs.

CMD Tracking Needs Improvement

The Army CIO did not appropriately track CMDs purchased as part of pilot and non-pilot programs. According to the Army CIO memorandum, "U.S. Army Guidance on Piloting Commercial Mobile Devices," November 3, 2011, Commands are required to obtain authorization from the Army CIO for all pilots using CMDs. However, Commands used

[2] Pilot CMDs are devices that test the feasibility of incorporating the use of CMDs into daily activities.

more than 14,000 CMDs without obtaining appropriate authorization from the Army CIO. For example, the CIO at USACE ERDC did not obtain authorization from the Army CIO for CMDs purchased as part of its pilot and non-pilot CMD programs. As a result, the Army CIO was unaware of 566 CMDs used by USACE ERDC. Furthermore, USMA did not obtain authorization for all CMDs purchased. Specifically, the Army CIO was aware of only 180 of 276 CMDs actually in use at USMA.

Commands used more than 14,000 CMDs without obtaining appropriate authorization from the Army CIO.

In addition to not obtaining the Army CIO authorization, CIOs at USMA and USACE ERDC did not obtain an interim authority to test. According to the DoD Information Assurance Certification and Accreditation Process, organizations must obtain an interim authority to test when live data are required to complete a specific test objective. However, CIOs at the two sites visited used live data, such as sensitive legal information at USMA and corporate e-mails at USACE ERDC, without obtaining an interim authority to test.

Furthermore, CIOs at USMA and USACE ERDC did not maintain an accurate accounting of CMDs. Specifically, they retained on their property books for CMDs that were lost, stolen, and damaged. Army Regulation 735-5, "Policies and Procedures for Property Accountability," states Commands should initiate a financial liability investigation of property loss when they identify lost, damaged, or destroyed property. The two sites visited did not always complete the financial liability investigation of property loss and report the devices to the Army CIO. For example, one MICA programmer at USACE ERDC damaged an iPhone and did not report the damage. Instead, the user replaced the device using personal funds and discarded the Government-issued device without the consent and knowledge of the Program Manager.

CMDs Not Consistently Configured

The Army CIO did not ensure that Army Commands and Components configured CMDs to adequately secure data stored on the device. DoD Directive 8500.01E, "Information Assurance," April 23, 2007, states that all IA and IA-enabled information technology products incorporated into DoD information systems will be configured in accordance with DoD approved security configuration guidelines and require a properly administered and protected password. Furthermore, according to the DoD CIO Memorandum, "Use of Commercial Mobile Devices in the Department of Defense," April 06, 2011, devices receiving or processing DoD information are considered part of a DoD information system and must be managed and controlled by an enterprise management system such as a mobile device management (MDM) application. MDM applications allow administrators to push security policies to manage devices and modify device configuration. However, at the two sites visited, CIOs at USMA and USACE ERDC did not use an MDM application to configure all CMDs. For example, the USMA CIO did not use an MDM application to configure 48 of 48 CMDs to require passwords. Instead,

15 of 48 CMDs did not require a password to access the device.

USMA officials relied on individual users to create passwords to unlock CMDs. As a result, 15 of 48 CMDs did not require a password to access the device.

In addition, the CIO at USACE ERDC did not use an MDM application to configure 62 of 62 non-pilot general research CMDs. USACE ERDC relied on individual users to configure non-pilot general research CMDs to require password for unlocking devices. As a result, users inconsistently configured passwords. Of the 62 non-pilot general research devices, 12 devices did not require a password to access the device. In addition, the Program Manager at USACE ERDC did not appropriately configure 71 of the 71 pilot CMDs managed by the AirWatch[3] MDM application. Although USACE ERDC used an MDM application for Blue Roof and MICA devices, it did not configure the MDM application to appropriately secure CMDs. As a result, passwords for Blue Roof and MICA pilot devices did not meet password complexity requirements.

Sanitization Requirements Did Not Exist

The Army CIO did not require all CMDs to be sanitized before transfer or after a device was lost, stolen, or damaged. The DoD CIO Memorandum, "Use of Commercial Mobile Devices in the Department of Defense," April 6, 2011, states that the system administrator will have the capability to transmit a remove data wipe command to the CMD. However, CIOs at USMA and USACE ERDC did not have the capability to remotely wipe all transferred, lost, stolen, or damaged CMDs. For example, the USMA Center for Faculty Excellence relied on users to reset the device to factory setting (a method of sanitization) before transferring to another user. As a result, 2 out of 48 CMDs still contained information from the previous user. Although USACE ERDC had the capability to remotely wipe CMDs used in the Blue Roof and MICA pilot programs using an MDM application, the CIO at USACE ERDC did not use an MDM application on the non-pilot general research CMDs. As a result, USACE ERDC could not wipe two devices stolen from a USACE ERDC employee's home.

Controls Lacking for CMDs Used as Removable Media

Cadets at USMA used CMDs as removable media to transfer and store sensitive case files and evidence related to Cadet Honor Committee hearings.

The Army CIO did not control CMDs used as removable media. The Army CIO Information Assurance Best Business Practice, "Control of Removable Media," February 29, 2012, requires Commands to strictly control removable media used to transfer personally identifiable information or public health information. CIOs at USMA and USACE ERDC did not adequately protect sensitive data stored on CMDs used as removable media. For example, cadets at USMA used CMDs as removable media to transfer and store sensitive case files and evidence related to Cadet Honor

[3] AirWatch allows administrators to establish baseline configurations to authenticate users, set security policies, protect personal and corporate data through encryption, prevent unauthorized device use, and perform monitoring and management functions.

Committee[4] hearings. Cadet investigators also used these CMDs as personal devices. The USMA CIO stated he was unaware that the devices were being used in this capacity. As a result, USMA did not implement the proper security controls to protect the sensitive investigative data stored on the devices. In addition, one user at USACE ERDC used a non-pilot CMD as removable media to transfer research documents and personally identifiable information from a networked computer.

CMD-Specific Training and User Agreements

The Army CIO did not require training and user agreements specific to CMDs. DoD Directive 8500.01E, "Information Assurance," April 23, 2007, requires the Army CIO to adequately train all personnel before authorizing access to DoD information systems. Additionally, the Defense Information Systems Agency, Smartphone Policy Security Technical Implementation Guide, Version 1, Release 6, November 23, 2011, provides a list of topics that users must receive training on before they are issued a CMD. Furthermore, the General Wireless Policy Security Technical Implementation Guide, Version 1, Release 7, November 23, 2011, requires users to sign a user agreement.

The CIO at USACE ERDC did not train CMD users outside of the Blue Roof and MICA pilot programs. Additionally, the CIO at USACE ERDC did not require pilot and non-pilot CMD users to sign a user agreement. Furthermore, the CIO at USMA did not have an IA training program specific to CMDs nor did they require users to sign a user agreement. For example, one user at USMA was unaware how to set up a password on the CMD. As a result, the user did not protect the device with a password.

Comprehensive Policy Specific to CMDs Needed

The Army CIO did not develop clear and comprehensive policy for CMDs purchased under pilot and non-pilot programs. Although the Army intended the current guidance to apply to all CMDs, the Army CIO specified requirements only for pilot programs and did not define what constitutes a CMD pilot program. The lack of clear and comprehensive guidance contributed to Army Commands not reporting and configuring CMDs to protect Army networks and data. As a result, risk increased that Army networks may become vulnerable to cybersecurity attacks and leakage of sensitive data. The Army CIO should develop clear and comprehensive policy to include requirements for reporting and tracking all CMDs purchased.

In addition, the Army CIO inappropriately concluded that CMDs were not connecting to Army networks and storing sensitive information. As a result, the Army CIO did not extend current IA requirements to the use of CMDs. The current Army CIO guidance for CMDs did not outline IA requirements for configuring and sanitizing CMDs, using CMDs as removable media, and completing training and user agreements. If the Army CIO does not extend current IA requirements to CMDs, risk increases that CMDs will be used to obtain unauthorized access to sensitive Army data. Therefore, the Army CIO

[4] The Cadet Honor Committee is a cadet-run group that investigates violations to the USMA honor code, such as cheating, lying, and stealing, and recommends potential punishment to the USMA Superintendent.

should designate CMDs as information systems, extend existing IA requirements to the use of all CMDs, and develop a process to verify that users of CMDs are following Army and DoD IA policies.

Army and Command CIOs Recognized Need for Change

As a result of our inquiries into the number of devices, the Army CIO stated that more Commands were reporting CMDs. The Army CIO indicated that accountability and tracking of CMDs has improved. In addition, On July 10, 2012, the CIO at USMA immediately directed the head of the Cadet Honor Committee to no longer allow cadet investigators to use CMDs as removable media to store sensitive data until USMA could configure the CMDs appropriately to protect case file information.

Furthermore, on August 28, 2012, the CIO at USACE ERDC issued an immediate moratorium on the acquisition of new CMDs. The moratorium stated that until USACE ERDC developed guidance and corrective action plan, personnel could not use Government funds to purchase CMDs. USACE ERDC recognized the need to use all aspects of AirWatch to manage and configure all CMDs. The CIO at USACE ERDC also began purchasing additional AirWatch licenses to ensure that all CMDs were appropriately managed and configured.

Conclusion

The Army CIO did not implement an effective cybersecurity program applicable to CMDs. Specifically, the Army CIO did not appropriately track more than 14,000 CMDs purchased as part of pilot and non-pilot programs. In addition, at the two sites visited, the Army CIO did not:

- ensure that Commands configured CMDs adequately to secure data stored on the device,
- require all CMDs to be sanitized before transfer or loss, and
- control CMDs used as removable media.

Without an effective cybersecurity program specific to CMDs, critical IA controls necessary to safeguard devices were not applied. As a result, the Army increased its risk of cybersecurity attacks and leakage of sensitive data.

Recommendations, Management Comments, and Our Response

We recommend that the Chief Information Officer, Department of the Army:

1. develop clear and comprehensive policy to include requirements for reporting and tracking all commercial mobile devices purchased under pilot and non-pilot programs.

Army Chief Information Officer Comments

The Director, Army CIO Cybersecurity Directorate, responding for the Army CIO agreed, stating the Army CIO Cybersecurity Directorate maintained a SharePoint Portal

and directed all Army organizations entering into a pilot to register and provide project documentation. Additionally, an Army Senior Leader with authority to accept risk for the designated organization must declare that guidance and policy is in place that aligns with the DoD Commercial Mobile Devices Implementation Plan. The Director also stated that the Army can access the Defense Information Systems Agency CONUS property management system, which accounts for every CMD assigned to the Army and that the system is used in the ongoing Defense Information Systems Agency Mobile Pilot. Furthermore, the Director stated that the Army Mobile Assurance Program Managers received and discussed this information during the Army Mobile Electronic Device Working Group meetings. The Director indicated that the Army CIO published guidance in November 2011 that directed Army organizations to register each pilot and document senior approval.

Our Response

We considered the comments from the Director to be nonresponsive. We found that Army Commands used more than 14,000 CMDs without receiving appropriate authorizations from the Army CIO. Of those devices, we identified 566 CMDs used by USACE ERDC and 96 CMDs at USMA that were not registered. Therefore, the SharePoint Portal would not be useful in accounting for the Army Commands using unregistered CMDs and devices that are not part of a pilot program. In addition, the current guidance published by the Army CIO inconsistently addressed CMDs registered in pilot programs only. The policy did not define what constitutes a pilot program, which resulted in the Army Commands not reporting and configuring CMDs appropriately. We request the Army CIO to provide comments to the final report.

2. designate commercial mobile devices as information systems and extend existing information assurance requirements to the use of commercial mobile devices.

Army Chief Information Officer Comments

The Director agreed with the recommendation, stating that users loosely apply designating CMDs as an information system. The Director also stated CMDs is considered an extension of that environment and did not require a separate designation and provides an interface into an existing system or environment. The Director stated that the Army, along with DoD and the Defense Information Systems Agency, are working to establish the ability to manage mobile devices utilizing an MDM system along with a Mobile Application Store. The Director stated that, in the end, DoD would be able to observe every managed mobile device and every application operating on these devices. According to the Director, the DoD memorandum on DoD Commercial Mobile Implementation Plan, dated February 2013, addresses this capability.

Our Response

We considered the comments from the Director to be nonresponsive. Without specific requirements to designate CMDs as information systems, users of CMDs would not apply the appropriate information assurance controls to protect the devices and the data contained on the devices. In addition, without a clear timeline on managing CMDs, there

is an increased risk that Army networks could be vulnerable to data leakage. We request that the Army CIO provide comments to the final report.

3. 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.

Army Chief Information Officer Comments

The Director agreed and stated that as the Defense Information Systems Agency and Army established the MDM and Mobile Application Store architectures that would make all CMDs managed mobile devices, which would result in the DoD and Army Service Provider having the ability to observe every DoD-managed CMD and the applications operating on the CMD. In addition, the Director stated that the Army would gain the ability to wipe or remove a device from the environment as well as monitor applications used, web sites visited, and data viewed, saved, or modified on the mobile devices. According to the Director, the Army issued a request for proposal for the MDM and Mobile Application Store and projected the determination of the award would be April 2013,initial operating capability expected by October 2013, and full operating capability being available before the end of FY 2014.

Our Response

The Director's comments were responsive. Therefore, no further comments are required.

Appendix. Scope and Methodology

We conducted this performance audit, from April 2012, through February 2013, 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.

We determined whether the Department of the Army had an effective cybersecurity program that identified and mitigated risks surrounding portable electronic devices and removable media. We limited our review to tablets and smartphones running on Apple iOS, Android, and Windows, mobile operating systems. We interviewed personnel in the Army CIO's office, DoD CIO's office, and the CIOs and users at USMA and USACE ERDC. In addition, we requested a list of in-scope CMDs used throughout the Army from October 1, 2010, through May 31, 2012. The Army CIO was unable to provide a complete list and provided only a list of Commands that had registered CMD pilot programs. As a result, we conducted a datacall from June 1, 2012, through July 27, 2012, requesting a list of all smartphones (excluding BlackBerry devices) and tablets procured. We received responses from the 3 major Commands, 6 of the 9 Service Component Commands, 9 of the 10 Direct Report Units, the Army Accessions Command, Army Cyber Command, and Eighth U.S. Army, totaling more than 14,000 devices. We selected USMA and USACE ERDC because these locations reported the highest number of CMDs.

We performed testing at USMA, West Point, New York, and USACE ERDC, Vicksburg, Mississippi, from July 2012 through August 2012. The DoD OIG statistician from the Quantitative Methods Division computed sample sizes using a 95 percent confidence level and a 10 percent precision rate. At USMA, we selected a statistical sample of 72 out of 276 CMDs. However, we were able to test only 48 CMDs because of device availability. At USACE ERDC, we selected a statistical sample of 71 out of 276 pilot CMDs and a statistical sample of 72 out of 290 general research CMDs. However, we were able to test only 71 pilot devices and 62 general research devices because of device availability. We were unable to project across the universe because of the incomplete universe and Commands lack of accountability.

We evaluated device security controls by reviewing inventory records, site policies, and procedures, and interviewing CMD users and other relevant personnel. In addition, we examined and tested CMD settings, such as password, operating system version, Bluetooth, and Wi-Fi to determine whether CMDs were configured or could be manipulated by users. We also reviewed MDM application security settings to determine whether CMDs were properly configured, when available. Specifically, the audit team obtained screenshots of the MDM application settings to determine whether devices had appropriate security settings.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Use of Technical Assistance

The DoD OIG's Quantitative Methods Division assisted with the audit by generating a sample of devices to test for each location using a 95 percent confidence level and a 10 percent precision rate. We obtained assistance from information assurance officers with the DoD OIG's Information Systems Directorate to create the testing steps. The information assurance officers reviewed the audit team's testing steps to ensure that the steps accurately tested relevant criteria.

Prior Coverage

During the last 5 years, the DoD Inspector General (DoD IG) has issued one report and the Army Audit Agency has issued one memorandum report related to Army CMDs. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm. Unrestricted Army reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/.

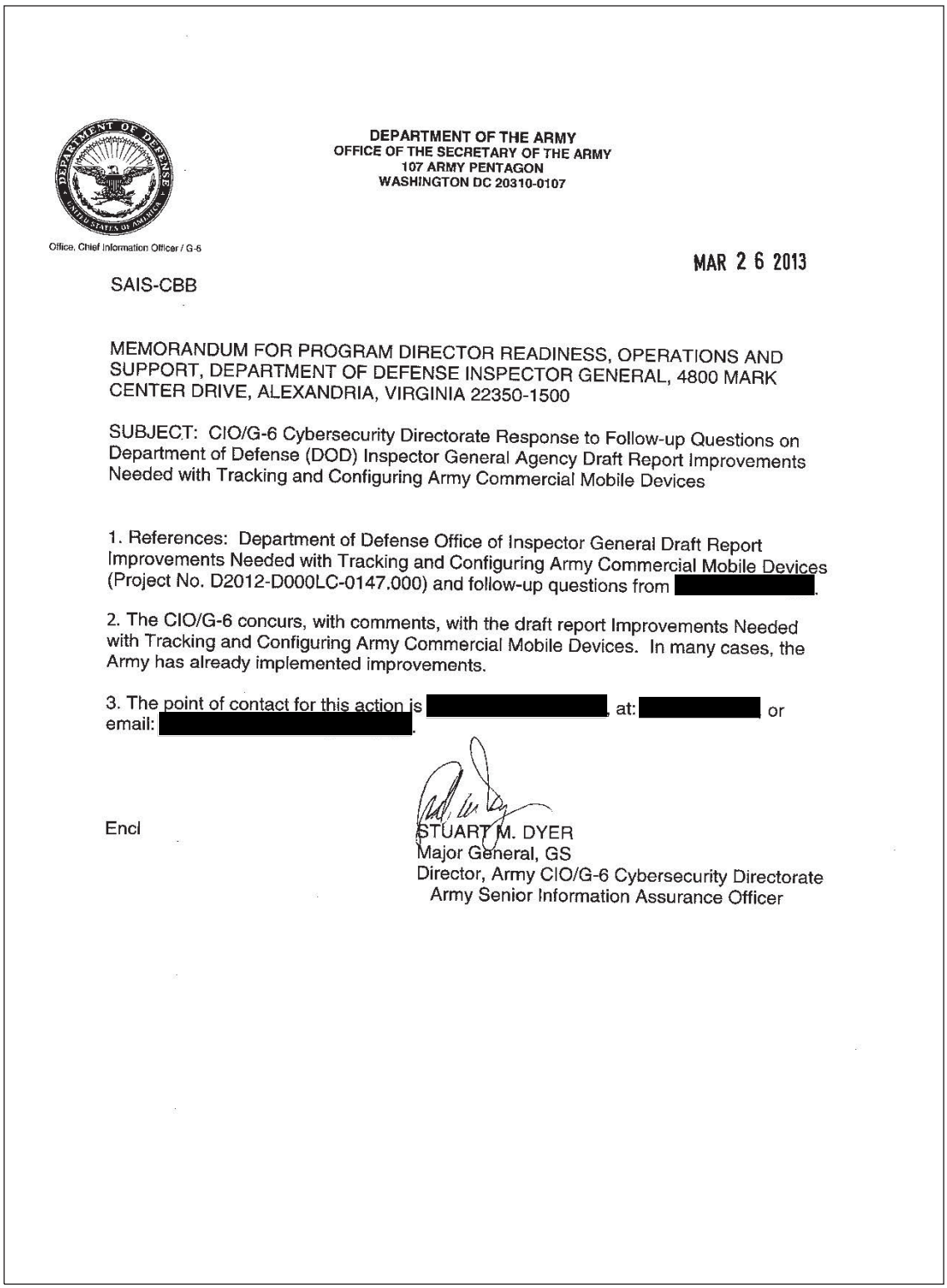
DoD IG

DoD IG Report No. D-2009-111, "Controls Over Information Contained in BlackBerry Devices Used Within DoD," September 25, 2009

Army Audit Agency

Army Audit Agency Memorandum Report No. A-2011-0215-IET, "The Army's Use of Smart Phones (Project Number A-2011-IET-0400.000)," September 29, 2011

Army Chief Information Officer Comments



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

Office, Chief Information Officer / G-6

MAR 2 6 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

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.

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.

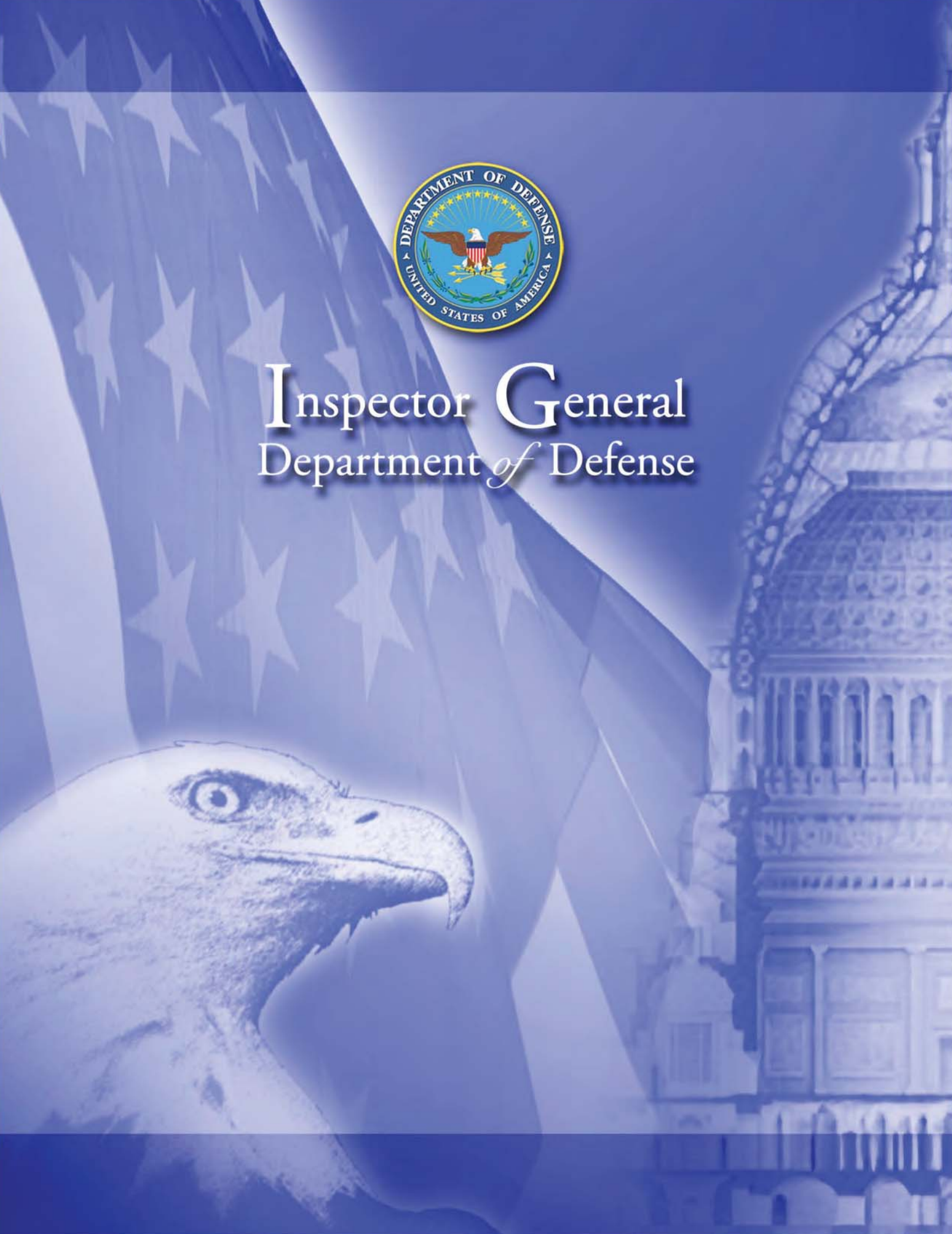
Chief Information Officer/G-6 Response:

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

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.



Inspector General
Department of Defense