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

Office, Chief Information Officer/G-6

SAIS-CB

SEP 1 1 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Guidance on the Use of Commercial Mobile Devices (CMD)

1. References:

a. Memorandum, Department of Defense Chief Information Officer (DoD CIO), 8 June 2012, subject: Department of Defense Mobile Strategy.

b. Memorandum, DoD CIO, 15 February 2013, subject: Department of Defense Commercial Mobile Device Implementation Plan.

c. Memorandum, DoD CIO, 21 March 2013, subject: Department of Defense Commercial Mobile Device Pilot Consolidation.

d. Army Regulation (AR) 25-1, 25 June 2013, subject: Army Information Technology.

e. AR 25-2, 23 March 2009, subject: Information Assurance, Rapid Action Revision.

f. Memorandum, Under Secretary of the Army, 10 May 2013, subject: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incidents.

g. Memorandum, Secretary of the Army, 11 March 2013, subject: Army Directive 2013-02 (Network 2020 and Beyond: The Way Ahead).

2. Purpose. This memorandum provides guidance for the use of all commercial mobile devices within the Army. Commercial mobile devices include wireless phones, smart phones and tablets. The unique combination of computing power, mobile applications and access to network and situational data (e.g., location, heading, speed) sets CMDs apart from other personal electronic devices, as defined in AR 25-2. This memorandum is based on DoD policy and applies to enterprise-connected as well as non-enterprise-connected devices, both of which are approved for use in the Army.

3. Enterprise Mobile Services. Army organizations must understand that mobility is considered an above-baseline service. Organizations that wish to utilize CMDs must pay the device costs, the wireless costs (voice and data), and the mobile device management costs for all existing devices and any new devices. All Army organizations electing to use CMDs will utilize enterprise mobile services to the greatest extent possible. The Army has

chosen the Defense Information Systems Agency (DISA) as the enterprise service provider for mobile services. DISA is currently implementing an enterprise mobile device management (MDM) system and an enterprise mobile application management (MAM) system. Any new CMD purchases must be listed on the Unified Capabilities Approved Products List, must utilize the Network Enterprise Technology Command blanket purchase agreement for wireless services, and must be managed by a DISA-approved MDM system.

4. Mobile Device Management and Mobile Application Management. All enterprise-connected devices will be managed by an approved MDM/MAM solution. The CIO/G-6 views DISA's enterprise MDM and MAM as key ingredients to extending existing information assurance controls to the use of commercial mobile devices. As they reach full operational capability, DISA and the Army will have the enterprise capability to manage every enterprise-connected CMD, as well as every application operating on an enterprise-connected CMD. Per DoD policy, the Army will coordinate with DoD to develop a consolidation plan that identifies which current CMD efforts should be merged or eliminated. Additionally, all organizations currently operating CMDs must develop a transition plan to move existing CMD activities to the DISA enterprise mobile capability as it becomes available.

5. Enterprise-Connected Devices. An enterprise-connected device is defined as a CMD that connects to a DoD network and is authorized to process and store up to Unclassified/For Official Use Only (FOUO) information and personally identifiable information (PII). For a CMD to be authorized for use as an enterprise-connected device, it must meet all of the requirements listed below. Devices that fail to meet all of these requirements will be designated as non-enterprise-connected devices.

a. Have the ability to sign and encrypt messages via Common Access Card/Public Key Infrastructure.

b. Be compliant with Federal Information Processing Standard 140-2 for data-at-rest and data-in-transit encryption, as well as compliant with all DISA security technical implementation guidelines (STIGs).

c. Be managed by an approved mobile device management system (described in paragraph 9 below) to enforce enterprise polices and wipe remotely if necessary.

6. Non-Enterprise-Connected Devices.

a. A non-enterprise-connected device is defined as a CMD that does not connect to a DoD network and is only authorized to store publicly releasable information.

b. Organizations operating non-enterprise-connected devices must manually configure CMDs to comply with the appropriate system security controls (in accordance with the references in paragraph 1 above) and must lock these configurations using an administrator password.

c. FOUO and PII information will not be stored on non-enterprise-connected devices. Organizations must inspect non-enterprise-connected devices quarterly for the presence of FOUO information or PII, and to ensure that security controls remain in place. The unit's Information Assurance Manager (IAM) will report any violations to CIO/G-6 for non-enterprise-connected devices. The MDM/Mobile Application Store solution will provide reports on violations for enterprise-connected devices once it is fully implemented. Units will comply with all current Army regulations. The responsibility for managing this process remains at the unit command level.

7. Commanders should use the Organizational Inspection Program, the Command Supply Discipline Program and staff assistance visits to help ensure unit adherence to CMD and information assurance policies. All organizations will continue to use existing property accountability regulations to ensure that CMDs are properly tracked.

8. User Responsibility. Users have a responsibility to handle information appropriately and commanders will hold users accountable for inappropriate behavior. IAMs are responsible for ensuring that CMD users receive training on CMD configuration and usage, and that they sign a user agreement prior to using a CMD. Commanders will follow the guidance provided in reference 1h.

9. Lost or Stolen Devices. A lost or stolen mobile device may provide access to sensitive information and resources within the enterprise network. This access could result in compromise of enterprise data or malicious activities executed via the mobile device. Immediately report the theft/loss of a mobile device to your IAM and chain of command. If the mobile device is unsecured and out of the immediate control of the assigned user, the user must report the device as lost or stolen. Time is of the essence. The sooner IA and security personnel are notified, the sooner protective measures can be executed. After notifying IA personnel, organizational leadership must initiate appropriate property accountability actions.

10. CMD Pilots. The Army CIO/G-6 will permit limited CMD pilots to test new technologies and techniques. The CIO/G-6 will track the pilots, share lessons learned, and prevent duplication of effort. The goal is to leverage CMD pilots and the DoD CMD strategy to support the development of the Army CMD strategy.

a. All CDM pilots must first receive authorization from the CIO/G-6. Any command or agency currently operating commercial mobile devices without an approved pilot or an Authority to Operate signed by the Enterprise Designated Approving Authority (DAA) must immediately identify its activities to the CIO/G-6 for approval. Requests for authorization to conduct a CMD pilot must be submitted to the CIO/G-6 Cybersecurity Directorate.

b. In order to protect Army and DoD data and networks, Information Assurance Program Managers will ensure that CMD pilots in their organizations are registered, authorized and compliant with this memorandum.

c. CMD pilots will operate for a limited time period designated at the start of the pilot; pilots may be extended with the approval of the CIO/G-6. At the end of the pilot, the CMD activity will either cease to operate or transition to production by following the Army's certification and accreditation process. All organizations currently operating CMD pilots must develop a transition plan to move existing CMD activities to the DISA enterprise mobile capability as it reaches full operational capability.

d. Pilots that intend to connect to a DoD network or to process sensitive, For Official Use Only or classified data on CMDs running an operating system not approved by the Enterprise DAA must abide by the following:

1) Have an Interim Authority to Test signed by the Enterprise DAA and a Certificate of Networthiness.

2) Ensure that applications used on CMDs are properly vetted in accordance with the references in paragraph 1 above.

3) Ensure that approved government applications are downloaded or pushed from a DoD- or Army-controlled site, not from a public marketplace.

11. The Army's long-term goal is to have a device-agnostic architecture employing comprehensive CMD solutions that comply with the Joint Information Environment, the Common Operating Environment Architecture and its Mobile Computing Environment. Additionally, use of commercial mobile devices must support the Army's Network 2020 and Beyond strategy.

12. Our adversaries are constantly looking for ways to exploit vulnerabilities in our technologies. As noted by the Secretary of the Army, the use of unapproved CMDs creates significant risk to the user, Army information and the entire enterprise. The CIO/G-6 is committed to providing CMD capabilities in a manner that properly addresses the associated risk, and your compliance and cooperation are essential. All Army leaders must join in the effort to manage and mitigate these risks by actively supporting the prohibition of unapproved devices. Just as with safety, we all are responsible for the security of our networks and ensuring the confidentiality, integrity and availability of our information and information systems.

13. The point of contact for this action is LTC Edward Mattison: (703) 545-1542 or edward.p.mattison.mil@mail.mil.

Susan S. Lawrence

SUSAN S. LAWRENCE
Lieutenant General, GS
Chief Information Officer/G-6

SAIS-CB
SUBJECT: U.S. Army Guidance on the Use of Commercial Mobile Devices

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade

CF:
Army Information Assurance Program Managers
Director, Army National Guard
Director of Business Transformation