



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

NOV 14 2011

MEMORANDUM FOR SEE DISTRIBUTION

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

1. References:

- a. Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, 25 May 2001
- b. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008
- c. AR 25-2, Information Assurance, 23 March 2009
- d. DoD Instruction 8420.01, subject: Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2009
- e. DoD Directive 8100.02, subject: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 23 April 2007
- f. DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
- g. DoD CIO Memorandum, Use of Commercial Mobile Device (CMD) in DoD, 6 April 2011
- h. DISA Windows Mobile 6-5 Secure Technical Implementation Guide (STIG), Version 1, Release 1, Updated 29 April 2011
- i. DISA phone ions Vulnerability and Risk Analysis, 20 May 2011
- j. DISA BlackBerry STIG, Version 1, Release 6, 28 July 2011
- k. Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, 1 October 2010

SAIS-CB

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

2. This memorandum provides guidance for conducting pilots of government issued Commercial Mobile Devices (CMD), e.g., tablets and smart phones. The unique combination of computing power, mobile applications (Apps), and access to network and situational data, e.g., geo-location, direction, speed, set CMDs apart from the other PEDs and requires specific guidance for their use. This memorandum does not supersede existing guidance regarding the introduction of mobile devices into Sensitive Compartmented Information Facilities (SCIF).

3. All pilots using CMDs must receive authorization from the CIO/G6. The CIO/G6 will track and share lessons learned and prevent duplication of effort. The CIO/G-6 intends to leverage CMD Pilots to support the development of the Army's mobile strategy. Information Assurance Program Managers (IAPMs) will ensure CMD pilots in their organizations are registered, authorized and compliant with this memorandum to ensure the protection of Army and DoD data and networks. Organizations must contact the Point of Contact (POC) in this memorandum and register their request for authorization to conduct a CMD Pilot at the following web address:
<https://intranet.hqda.pentagon.mil/ciog6/cyber/projmgmt/med/Pilots/Forms/AllItems.aspx>.

4. Pilots desiring to connect to Army networks or process sensitive, For Official Use Only (FOUO), or classified data on CMDs running an operating system not approved by the Enterprise Designated Approval Authority (DAA) must abide by the following:

a. Have an Interim Authority to Test (IATT) and Certificate of Networkiness (CON) in accordance with (IAW) references in paragraph 1 above.

b. Ensure Apps used on CMDs are properly vetted IAW references in paragraph 1 above.

c. Ensure approved government Apps are downloaded or pushed from a DoD or Army controlled site, not from a public marketplace.

5. The Army's long-term goal is to have a device agnostic architecture employing comprehensive CMD solutions that comply with the Common Operating Environment (COE) Architecture and its Mobile Computing Environment (CE). The Assistant Secretary of the Army for Acquisition, Logistics and Technology [ASA (ALT)] Mobile CE working group is leading the effort to identify standards for the following criteria:

a. FIPS 140-2. Use proper strength of encryption algorithms for data at rest and data in transit.

b. Common Access Card (CAC) / Public Key Infrastructure (PKI). Support CAC/PKI capabilities for two-factor authentication to Army networks and websites. Additionally, leverage CAC/PKI for signing and encrypting emails.

SAIS-CB

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

c. Data at Rest (DAR). Ensure sensitive information is encrypted IAW references in paragraph 1 above for data stored on the CMD. An alternative approach is, not to store data on the device, i.e., thin client.

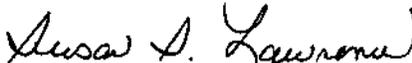
d. Mobile Device Management (MDM). Ensure enterprise policy management is available for all CMDs, e.g., asset visibility, device patching, and anti-virus updates similar to current desktop management capabilities. A currently fielded example would be Blackberries under the Blackberry Enterprise Server (BES) and Blackberry Administration Service (BAS).

e. Applications. Include standard applications for the CMD, e.g., Enterprise Email, and its associated DoD Identity Synchronization Service (IdSS) and the approved Software Development Kit (SDK), reusable software code and guides needed to develop new applications.

6. Over this past year, there has been a great deal of effort directed at evaluating CMDs and establishing the Army Software Marketplace. As new CMDs are approved, they will be made available via the Computer Hardware Enterprise Services and Software (CHESS) website, <https://chess.army.mil>, and the DoD Unified Capabilities Approved Products List (UC APL) website, <https://aplits.disa.mil/processAPList.do>. Organizations using CMDs need to ensure appropriate support plans are in place for operations and maintenance costs, technical support agreements, and use the Army's Software Marketplace to develop new Apps.

7. I am committed to providing these capabilities in a manner that properly addresses the associated risk. Our adversaries are constantly looking for ways to exploit vulnerabilities in our technologies. The use of unapproved CMDs creates significant risk to the user, Army information and to the entire enterprise. As leaders, it is our responsibility to manage these risks. Together we are responsible for the security of our networks to ensure the confidentiality, integrity and availability of our information and information systems.

8. The POC is LTC Matthew Dosmann, (703) 545-1743, cio-g6.cyber.inbox@mail.mil.


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

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

SAIS-CB

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

COMMANDER

US ARMY FORCES COMMAND

US ARMY TRAINING AND DOCTRINE COMMAND

US ARMY MATERIEL COMMAND

US ARMY EUROPE AND SEVENTH ARMY

US ARMY CENTRAL

US ARMY NORTH

US ARMY SOUTH

US ARMY PACIFIC

US ARMY SPECIAL OPERATIONS COMMAND

US ARMY AFRICA

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND

US ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC
COMMAND

EIGHTH US ARMY

US ARMY CYBER COMMAND/2ND ARMY

US ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL
COMMAND (ARMY)

US ARMY MEDICAL COMMAND

US ARMY INTELLIGENCE AND SECURITY COMMAND

US ARMY CRIMINAL INVESTIGATION COMMAND

US ARMY CORPS OF ENGINEERS

US ARMY MILITARY DISTRICT OF WASHINGTON

US ARMY TEST AND EVALUATION COMMAND

US ARMY RESERVE COMMAND

US ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY

DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER

DIRECTOR, ARMY NATIONAL GUARD

CF:

ARMY INFORMATION ASSURANCE PROGRAM MANAGERS