



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JAN 17 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Commercial Mobile Device (CMD) Interim Policy

Reference: DoD CIO Memo, "Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD)", April 6, 2011

For reference memo addressed the increasing dependency and challenges presented by emerging commercial mobile technologies and provided security objectives for the limited use of CMDs that connect to DoD networks or process DoD information. This memorandum defines interim policy and establishes responsibilities to increase mission capabilities of CMDs while adhering to DoD security policies. It does not obviate or supersede current DoD standards for physical security, confidentiality, integrity, or availability. Combatant Command/Service/Agency CIOs still hold the responsibility of making a risk-based determination prior to authorizing CMD implementations based on this memorandum.

Attachment 1 addresses configuring optional security settings in the BlackBerry Security Technical Implementation Guide to improve user acceptance and functionality. Attachment 2 discusses requirements for the use of non-enterprise activated CMDs. Attachment 3 outlines interim steps to support CMD applications in the DoD. Attachment 4 lists definitions used in this memorandum.

The DoD CIO point of contact for this matter is Mr. Mark Norton at email: mark.norton@osd.mil, (703) 607-0711.

A handwritten signature in black ink, appearing to read "Teresa M. Takai".

Teresa M. Takai

Attachments:
As stated

BlackBerry STIG Optional Security Setting Modifications

1.1. PURPOSE

The required and recommended BlackBerry IT policies defined in the BlackBerry Security Technical Implementation Guide (STIG) along with the use of older BlackBerry devices has increased demand for commercial mobile devices (CMD) running the iOS or Android platforms. Prior to making a significant investment in supporting one or more new platforms, it is important to consider that the BlackBerry STIG includes recommended optional settings that can be modified to provide additional functionality with authorization from Combatant Command/Service/Agency (CC/S/A) CIOs.

CC/S/A CIOs should consider the impacts from any malicious modification of the BlackBerry device that negates intended security controls. Such a determination shall assume the intentional modification exposes all data processed by the BlackBerry device to unintended users and will be a factor in where the BlackBerry device may be used and what data it may process. In certain cases, these capabilities could significantly enhance mission effectiveness and user satisfaction for little additional cost. Enabling additional capabilities does not relieve the user from observing OPSEC best practices or existing policy. While this attachment focuses on BlackBerry device deployments, the same methodology may apply for future CMD STIGs.

1.2. POLICY

To enhance mission effectiveness, minimize costs, and promote security:

1.2.1. Optional security settings in the default BlackBerry STIG configuration may be changed after a risk-based determination by the CC/S/A CIO.

1.2.2. Optional security settings in the BlackBerry STIG may be modified for individuals or groups of users to enable some or all of the following additional functionality:

1.2.2.1. Camera and Video Recorder

1.2.2.2. External memory

1.2.2.3. Podcast downloads

1.2.2.4. Real Simple Syndication (RSS)

1.2.2.5. Global Positioning System (GPS)

1.2.2.6. Social networking

1.2.2.7. Allow caller ID to show names of contacts in device address book

1.2.2.8. Additional functionality may be enabled by CC/S/A CIO direction after conducting a risk-based determination.

1.2.3. Users of BlackBerry devices with modified optional security settings shall complete annual Operations Security (OPSEC) training relating to their configuration.

1.3. RESPONSIBILITIES

1.3.1. Each CC/S/A shall identify desired functionality on deployed BlackBerry devices and develop BlackBerry IT policy configurations as discussed in section 1.2.

1.3.2. CC/S/A CIOs shall make a risk-based determination to deploy these enhanced BlackBerry IT policy configurations to individuals or groups of users. CIOs who require additional information shall contact the Defense Information Systems Agency Field Support Office.

1.3.3. CC/S/A's shall update existing OPSEC training or develop, offer, and maintain OPSEC training for each enhanced BlackBerry IT policy configuration.

Use of Non-Enterprise Activated CMDs for DoD tasks

2.1. PURPOSE

This attachment promotes the discovery of enhanced mission efficiencies through the use of non-enterprise activated commercial mobile devices (CMD). As the DoD works with industry to identify defense in depth capabilities to meet existing DoD security policies on CMDs, each Combatant Command/Service/Agency (CC/S/A) is authorized to use non-enterprise activated CMDs for DoD tasks involving only non-sensitive information when meeting the policy contained in this attachment. The policy in this attachment does not apply to CMDs that are configured in accordance with approved guidance for enterprise connectivity. CC/S/A CIOs must determine authorized DoD tasks that can be performed with non-enterprise activated CMDs, but examples of tasks that could be performed include:

- 2.1.1. Conducting user training
- 2.1.2. Reviewing CC/S/A CIO authorized operational tutorials
- 2.1.3. Monitoring of meteorological data
- 2.1.4. Viewing flight maps
- 2.1.5. CC/S/A recruiting activities

2.2. POLICY

To conduct authorized DoD tasks using non-enterprise activated CMDs:

2.2.1. Non-enterprise activated CMDs and specific security solutions shall be listed on the DoD Unified Capabilities (UC) approved products list (APL) with version information (located at <http://gccs.disa.mil/ucco/>) under multi-function mobile device use case #1 per the UC Requirements document.

2.2.2. Non-enterprise activated CMDs shall only process or store non-sensitive information.

2.2.3. Non-enterprise activated CMDs shall not use DoD-issued software certificates.

2.2.4. Non-enterprise activated CMDs that are not government owned shall require CC/S/A CIO approval and the signature of a forfeiture agreement by the user.

2.2.5. Non-enterprise activated CMDs shall follow existing policy when accessing web-based services authorized for external access, which store sensitive DoD information. CC/S/A's are encouraged to implement technical controls that prevent sensitive DoD information from being downloaded and stored.

2.2.6. Non-enterprise activated CMDs shall not process or store official DoD email. Access to DoD webmail services shall follow policy statement 2.2.5.

2.2.7. Non-enterprise activated CMDs shall not physically or wirelessly connect directly to DoD workstations (e.g. NIPRNET or SIPRNET) or other CMDs with sensitive DoD information.

2.2.8. Non-sensitive information shall only be transferred to and from non-enterprise activated CMDs using the public Internet or a CIO designated workstation that only connects to a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means.

2.2.9. All non-enterprise activated CMD users shall sign a DoD user agreement. This agreement shall include additional terms that define the CIO authorized tasks for that CMD and the authorized CMD applications.

2.2.10. All non-enterprise activated CMD users shall complete Operational Security (OPSEC) training that provides use guidelines and vulnerability mitigation techniques.

2.2.11. Only CMD applications approved by the CIO, after a risk-based determination, shall be installed on non-enterprise activated CMDs.

2.2.12. Non-enterprise activated CMDs shall require a passcode consistent with the requirements defined in the General Mobile OS (Non-Enterprise Activated) STIG referenced in 2.3.1 below.

2.2.13. Non-enterprise activated CMDs should be manually audited by a system administrator periodically in person to determine if unauthorized software is or has been running on the device or if the device OS has been modified (e.g. rooted or jailbroken) when centralized over-the-air auditing is unavailable.

2.2.14. Centralized policy enforcement should be considered from a DMZ that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means to:

2.2.14.1. Enforce non-enterprise activated CMD application installation or removal requirements consistent with policy statement 2.2.11 of this attachment.

2.2.14.2. Enforce non-enterprise activated CMD password requirements consistent with policy statement 2.2.12 of this attachment.

2.2.14.3. Detect or prevent OS/firmware modification. (e.g., rooting or jailbreaking)

2.2.14.4. Audit installed applications based on CIO approved configuration list.

2.3. RESPONSIBILITIES

2.3.1. Within 30 days of the signature of this memorandum the Director, DISA shall develop a General Mobile OS (Non-Enterprise Activated) STIG.

2.3.2. CC/S/As shall propose specific CMDs and specific security solutions to DISA for inclusion on the UC APL under multi-function mobile device use case #1 by contacting ucco@disa.mil or following instructions listed at <http://www.disa.mil/Services/Network-Services/UCCO>.

2.3.3. Within 120 days of the signature of this memorandum the CC/S/As shall develop OPSEC training specifically for the use of non-enterprise activated CMDs, update existing training to include use of non-enterprise activated CMDs, or leverage existing CMD training on IASE (<http://iase.disa.mil>).

Support for CMD Applications

3.1. PURPOSE

CMD applications can enhance user productivity, but also provide security and interoperability risks. Due to the growing proliferation of CMD applications, it is necessary to establish an interim list of approved CMD applications as well as interim CMD application security evaluation criteria and application development requirements. This will help ensure that applications developed and/or used by the DoD meet security and interoperability requirements. This attachment does not address all the requirements for supporting CMD applications, but future policy will address additional topics such as specific requirements for a centralized CMD application store.

3.2. POLICY

To support the use of CMD applications in the DoD:

3.2.1. All CMD applications shall be assessed using DoD security evaluation criteria upon completion as referenced in 3.3.1.1 below.

3.2.2. All DoD approved CMD applications shall be centrally listed on <http://iase.disa.mil>.

3.2.3. All DoD developed CMD applications shall meet the DoD interoperable CMD application development requirements upon completion as referenced in 3.3.2 below.

3.3. RESPONSIBILITIES

3.3.1. Within 90 days of the signature of this memorandum the Director, DISA shall:

3.3.1.1. Define security evaluation criteria for CMD applications and submit to the DoD CIO for approval.

3.3.1.2. Upon approval by the DoD CIO, publish the security evaluation criteria to <http://iase.disa.mil>.

3.3.1.3. Publish and maintain a list of approved CMD applications on <http://iase.disa.mil> that includes instructions on how to obtain the CMD application and supporting risk-based determination documentation.

3.3.2. Within 90 days of the signature of this memorandum the CIO of the Army shall coordinate with the CMD Working Group and the CC/S/As to define interoperable CMD application development requirements consistent with existing DoD policies. A document shall be submitted to the DoD CIO for approval defining:

3.3.2.1. Recommended CMD application development languages or frameworks that minimize CMD application development across multiple devices (e.g. OZONE Widget Framework, JavaScript, .NET and HTML5).

3.3.2.2. Recommended CMD application software development kits, environments, and libraries that promote interoperability and security.

3.3.2.3. Required protocols and standards relevant to networking, authentication, encryption, and data exchange.

3.3.2.4. Necessary application programming interfaces to control network interfaces and peripherals including, but not limited to camera(s), GPS, Wi-Fi, Bluetooth, Cellular, and Near Field Communication.

3.3.2.5. Constraints or requirements for synchronization of data or backups with enterprise and commercial cloud services.

Definitions

4.1. Commercial Mobile Device (CMD). A subset of portable electronic devices (PED) as defined in DoDD 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (Touch Screen, Miniature Keyboard, etc.) and exclude PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers.

4.2. CMD Application. Software that runs on CMDs according to permissions granted by the user upon installation and is commonly known as “apps” by the consumer industry.

4.3. Non-Enterprise Activated CMD. A CMD that does not store credentials used to login to a DoD network or information system, is not configured to process or store email from a DoD electronic messaging system, and is not centrally controlled or monitored from a DoD network.

4.4. Non-Sensitive Information. Information available in the public domain or DoD information that has been approved for public release.

4.5. Portable Electronic Device (from DoDD 8100.02). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, and hand-held/laptop computers.