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

CHIEF INFORMATION OFFICER

APR 0 6 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT 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: Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD)

CMDs (e.g. smartphones, e-readers, tablets, etc.) offer unprecedented opportunities for advanced mobile computing and communications. Yet our increasing dependency on rapidly emerging commercial technologies adds a new element of risk to DoD information. Therefore, this memorandum emphasizes the importance of adhering to existing security policies while the department moves forward to overcome today's digital challenges. The attached security objectives for CMDs outline current challenges and provide potential mitigations for limited use pilots and mission critical applications. The follow-on actions support our long-term objectives and will be incorporated into the updated DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 23, 2007. The DoD enterprise strategy will be developed in a phased approach as CMD standards, accreditation processes, device compatibility, and software/applications evolve. DoD CIO has established a CMD Working Group (CMDWG) to conduct technology assessments and establish efficient procurement practices.

My point of contact for this matter is Dr. Rocky Young at email: robert.young@osd.mil, 703-602-9926.

Teresa M. Takai
Acting

Attachment:
As stated

SECURITY POLICY REVIEW AND OBJECTIVES FOR COMMERCIAL MOBILE DEVICES (CMD)

References:
(a) DoD Directive (DoDD) 8100.02, ”Use of Commercial Wireless Devices, Services, and Technologies in the DoD GIG,” April 23, 2007
(b) DoD Instruction (DoDI) 8420.01, “Use of Commercial Wireless Local-Area Network (WLAN) Devices, Systems and Technologies,” November 03, 2009
(c) DoDD 8500.01E, “Information Assurance (IA),” April 23, 2007
(d) DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007
(e) National Security Telecommunications and Information Systems Security (NSTISS) TEMPEST/2-95, December 12, 1995
(f) Director of Central Intelligence Directive (DCID) 6/9, November 18, 2002

Reference (a) establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the department. References (b) through (f) identify additional requirements which affect the use of mobile capabilities within the DoD. The Defense IA Security Accreditation Working Group (DSAWG), which adjudicates community risk and approves Security Technical Implementation Guides (STIGs), recently reviewed a CMD Operating System and determined these devices are not yet suitable for wide-scale DoD deployment.

Component CIOs should thoroughly review the security requirements and consider the potential mitigations listed below before granting limited-use IATOs for devices with no currently approved STIG. Copies of IATOs, best practices, and results from completed or ongoing Component-level pilots and assessments should be forwarded to the DoD CIO Commercial Mobile Device Working Group (CMDWG) for community sharing in support of this effort. The DoD CIO is actively working with CMD and third party vendors to identify appropriate mobility solutions. Significant requirements and potential mitigations for limited-use employment of CMDs are listed below along with examples of ongoing efforts to overcome current security challenges.

1. Enterprise Management: Devices receiving and/or processing DoD Information are considered part of a DoD Information System (IS), therefore the devices must be managed and controlled by an enterprise management system, for example: Email redirection from the email server (e.g., Exchange Server) to the device shall be controlled via centrally managed server; desktop or Internet controlled email redirection is not authorized; the system administrator shall have the capability to configure the device browser to connect only to a specific URL (e.g., DoD network VPN gateway or DoD web proxy) during provisioning of the mobile device; the system administrator shall have the capability of performing a device audit; and the user shall not be able to override security configurations.

a. Potential Mitigation:

1) Conduct periodic manual and automated auditing of CMDs, not to exceed 90 days, to ensure system components, software applications, and settings are maintained according to intended use and no new software applications have been installed.

2) CMD access to DoD networks will be limited via controlled access gateways.

b. Follow-on Actions:

1) DISA will identify or assess and report progress toward identifying appropriate auditing options within 30 days.

2) DISA and NSA will identify or assess and report progress toward identifying appropriate access gateway(s) within 30 days.

2. Data Protection: Encryption of sensitive DoD data transmissions (data-in-transit or DIT) to and from mobile devices and data-at-rest (DAR) on mobile devices is required. The validated encryption module must be implemented in accordance with the Cryptographic Module Validation Program (CMVP) per Federal Information Processing Standards (FIPS) Publication 140-2, for example: All data stored on the device will be encrypted using a FIPS validated module; a password must be successfully entered before the device data is unencrypted; and when a screen lock occurs (user initiated or due to an inactivity timeout) all data will be re-encrypted; the system administrator shall have the capability to transmit a remote Data Protection (e.g. Data Wipe or Data Obfuscation) command to the handheld device.

a. Potential Mitigation: Maintain DIT and DAR encryption either through a DoD-approved Operating System software application, or a DoD-approved third party secure partition environment/application.

b. Follow-on Actions: DISA and the DoD CIO will assess the status of vendor progress toward achieving FIPS 140-2 validation and will ensure the appropriate STIGs are updated as encryption module validation is achieved.

3. Access Control: Devices must conform to DoD IS standards for access control, for example: DoD approved identification and authentication to mobile devices is required; CMDs should employ approved user credentials to authenticate to DoD information systems such as DoD web servers, collaboration tools, and data files.

a. Potential Mitigation: Implement mutual authentication at the device and network levels in accordance with the FIPS 140-2 standard. Direct access to network resources (e.g. file servers) shall continue to be restricted until approved identification and authentication controls are in place.

b. Follow-on Actions: DISA will identify or assess and report progress toward identifying appropriate access control options within 30 days.

4. DoD Public Key Infrastructure (PKI) Credentials: Devices must implement DoD PKI Standards or approved authentication credentials. For example: mobile email management servers will be configured to disable connections from the device to any back office server unless explicitly approved; email on CMDs will be capable of using public key enabled digital certificates for authentication between the device and the server; the system administrator shall

have the capability to enable or disable PKI-related configuration settings on the handheld device or server or alternatively; the system will automatically provide the user the capability to accept or not accept a certificate with specific characteristics (Note: the desire is to give the user the same capabilities enabled on DoD workstations).

a. Potential Mitigation: All devices transferring sensitive DoD information must be enabled to send and receive signed, and/or encrypted messages using DoD PKI credentials.

b. Follow-on Action: DISA and the DoD PKI office will identify or assess and report progress toward identifying appropriate PKI options within 30 days.

5. Software/Applications: Software and applications must be installed from an approved source, for example: all applications must be DAA-approved and have a risk assessment completed prior to deployment; a trusted loading process must be the foundation for device provisioning (whether tethered or over-the-air (OTA)); and the trusted OTA provisioning process must provide mutual authentication between the provisioning server and device while providing for data confidentiality, integrity and availability.

a. Potential Mitigation: Software applications developed for CMDs shall be installed under control of the organization and from an approved source.

b. Follow-on Actions: DISA will develop appropriate application management procedures and provide the initial draft within 90 days.

6. Training: The rapid evolution of new CMDs and the current dependence on user-based security controls introduce risks to the environment requiring more robust system administrator and user training and awareness.

a. Potential Mitigation: Conduct OPSEC awareness and CMD security procedures locally.

b. Follow-on Action: DISA will review and as necessary update appropriate information assurance training to include the emerging risks introduced by CMDs.