DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Chief Information Assurance Executive (CIAE) 3 May 2013

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense Mobility Governance

Reference: Department of Defense Chief Information Officer Memorandum, "Department of Defense Commercial Mobile Device Implementation Plan," February 15, 2013

1. Department of Defense (DoD) Commercial Mobile Device (CMD) Implementation Plan establishes the framework to equip users and managers with mobile solutions that leverage commercial off-the-shelf products, improve functionality, decrease cost, and enable increased personal productivity. The CMD Implementation Plan tasks DISA to "define and publish a methodology for connecting CMDs via approved commercial carrier services to DoD networks", "develop and publish guidance for mobile application management and certification processes", and to "modify the security approval process for mobile devices, Operating Systems, and applications to ensure that DoD will have access to the latest mobile technologies in a timely manner by maximizing vendor participation."

2. Under the authority of DoD CMD Implementation Plan, DISA hereby releases the Department of Defense Mobility Governance for immediate use as a DoD-approved CMD security and enterprise mobile application approval process.

3. Questions regarding this governance should be addressed to disa.meade.ciae.list.ae22-cyber-assurance-branch@mail.mil, phone number (301) 225-7900.

5/3/2013

X Mark S Orndorff

MARK S. ORNDORFF
Chief Information Assurance Executive and Prog...
Signed by: ORNDORFF.MARK.STEPHEN.1045813610

1 Enclosure:
DoD Mobility Governance
subj as above, 3 May 13

SUBJECT: DEPARTMENT OF DEFENSE MOBILITY GOVERNANCE

References: (a) DoD CIO Memo, "Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD)," April 6, 2011
(b) DoD CIO Memo, "DoD Commercial Mobile Device (CMD) Implementation Plan," February 15, 2013
(c) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as amended
(d) DoDI 8420.01, "Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies," November 3, 2009
(e) DoD CIO Memo, "Commercial Mobile Device (CMD) Implementation Plan" February 15, 2013
(f) DoD Directive 8500.01E, "Information Assurance (IA), April 23, 2007"
(g) DoD Instruction 8100.04, "DoD Unified Capabilities, December 9, 2010"
(h) CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, December 15, 2008
(i) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012
(j) CNSSD 505, "Supply Chain Risk Management," March 7, 2012

Background: The DoD CIO Memo, "DoD Commercial Mobile Device (CMD) Implementation Plan," establishes policy and assigns responsibilities for the acquisition, implementation, and operation of CMD technologies for DoD operations. Additionally, the DoD CIO Memo states that DoD shall: institute policies and standards to ensure the secure adoption and proper use of mobile devices and related support infrastructure; and that the policies and standards shall support the fluid and dynamic nature of mobile technology; enable timely deployment; and provide a means for robust management and control. The DoD Mobility Governance was developed to address those roles and responsibilities assigned to the DoD Components. The Mobility Governance will continue to evolve as the mobile technologies mature.

1. Purpose: Outline DoD's Mobility Governance processes, roles, and responsibilities for the unclassified environment that:

a. Assign the roles and responsibilities for DoD's Mobility enterprise services implementation and operations.
b. Provide the process for agile and adaptive development, deployment, and implementation of secure and interoperable mobile devices, operating systems, and applications.
c. Provide a means for robust management and control of the mobile environment.

2. Roles and Responsibilities:

2.1 DISA will:

2.1.1 Develop and maintain an enterprise Mobile Device Management (MDM) service platform.
2.1.2 Develop, operate, and maintain a controlled-access, tiered (e.g., user-end, enterprise, database) MAS to serve as a central repository for certified mobile applications.
2.1.3 Publish guidance for development of mobile applications to promote interoperability across CMD platforms, extensibility, and code reuse.
2.1.4 Develop and publish Mobile Security Requirements Guides (SRG) to provide configuration guidance for proper implementation of CMDs within DoD networks, including device hardening techniques.
2.1.5 Establish a streamlined CMD security approval process with the objective of a 90-day approval cycle for mobile devices and mobile OSs. The approval process for mobile devices will work toward a device-agnostic approach.
2.1.6 Establish and maintain a qualified product list of CMDs that may be connected to DoD networks in accordance with DoD policy.
2.1.7 Establish a risk based GIG Flag Panel approved streamlined enterprise mobile application approval process.
2.1.8 Approve Secure Technical Implementation Guide‘s (STIG) for DoD use in securing CMDs.

2.2 DoD Components will:

2.2.1 Develop convergence plans to integrate any MDM or MAS instantiation efforts into the DoD enterprise capability.
2.2.2 Develop application development and management guidelines, certification processes, and sustainment capability consistent with DoD guidance.
2.2.3 Provide a list of approved CMD applications, instructions on how to obtain the applications, descriptions of the function of applications sufficient to avoid duplication, and supporting risk-based determination documentation to the DISA Mobility PMO and make the applications available to the Enterprise MAS.
2.2.4 Download completed and approved mobile applications from the enterprise and/or DoD Component MASs.
2.2.5 Deploy mobile solutions that will utilize the approved CMD, OS, and mobile applications processes.
2.2.6 Perform Supply Chain Risk Assessment for CMDs, and mobile applications.
2.2.7 Apply the Mobile Application SRG for mobile application testing.

3. Process. The process workflows outlined below provide guidance for the agile and adaptive delivery of secure and interoperable mobile devices and operating systems into the DoD environment; and promote the development/approval and use of mobile applications to quickly deliver function to DoD mobile device users in a secure and interoperable manner.

a. Commercial Mobile Devices and Operating Systems: DoD's acquisition of commercial mobile devices will include a requirement for carriers supporting mobile devices to provide evidence of compliance with the DoD Mobile Security Requirements Guides (SRG) via the development of a product specific STIG based on the appropriate Mobile SRG. The intent is for carriers to include the security requirements outlined in the SRG as part of their normal device and software review and approval processes. Figure 3.1 outlines the process for the agile and adaptive delivery of secure mobile device operating systems into the DoD environment.

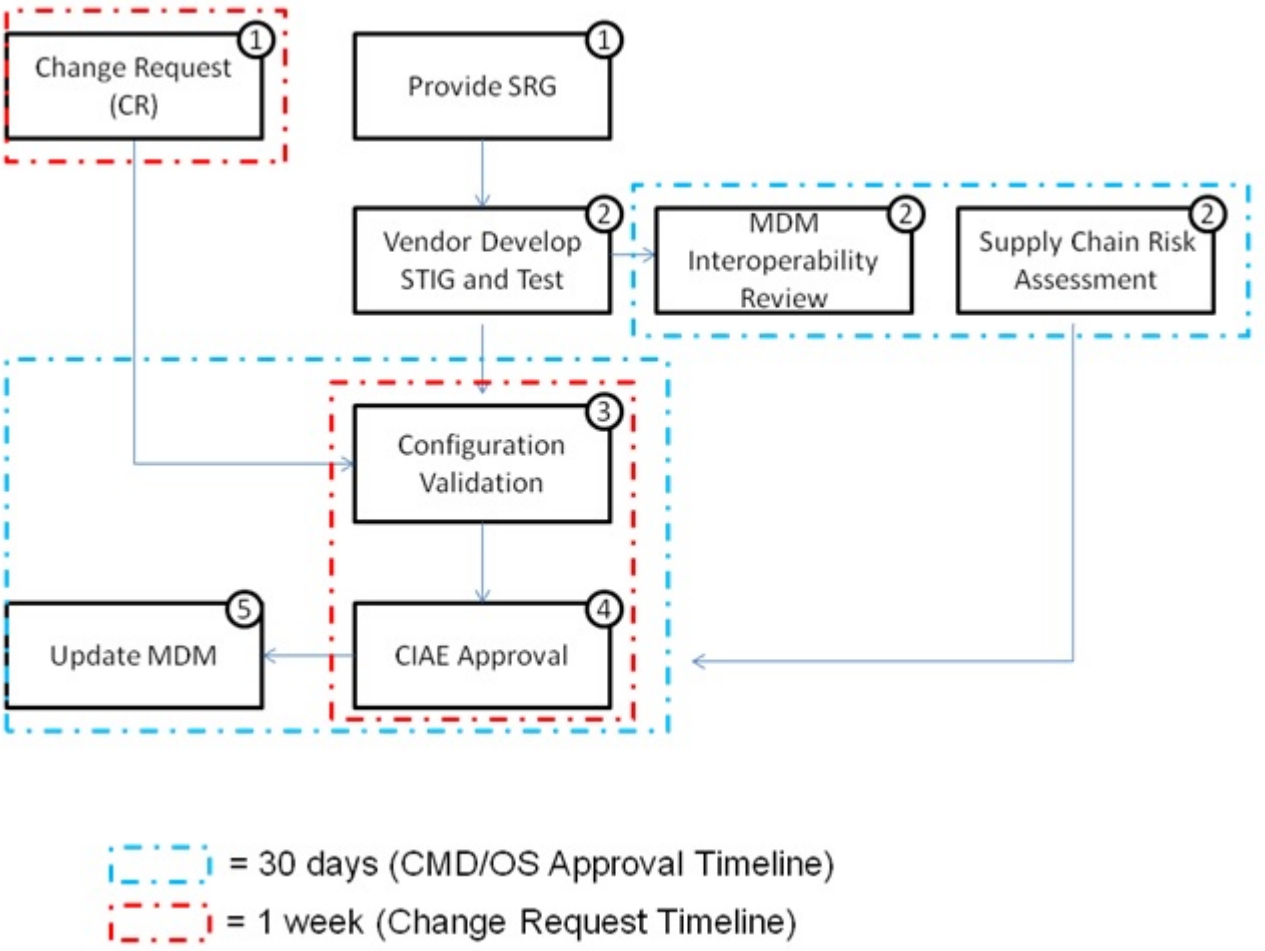

Figure 3.1 Commercial Mobile Devices and O/S Process

(1) Step 1: Vendor and government sponsor submits a Security Technical Implementation Guide (STIG) development request to DISA Field Security Operations (FSO). The FSO provides the Security Requirements Guides (SRGs) and STIG Template to the vendor. For Change Requests (CR), a CR template is filled out and sent to the DISA Mobility PMO for CA/DAA approval.

(2) Step 2a: The vendor will develop and test the requisite STIG. FSO will coordinate with the DISA Mobility PMO to determine the priority of reviewing vendor submitted STIGs.

(3) Step 2b: In parallel, the Mobility PMO tests and verifies MAS and SRG requirements can be enforced using the MDM. The MDM integration results are provided to the DISA FSO for review.

(4) Step 2c: Also in parallel, the Mobility PMO will give the CMD/OS information to DISA CIAE for Supply Chain Risk Assessment.

(5) Step 3: FSO evaluates the vendor STIG, validating that the STIG appropriately addresses the SRG requirements, and identifies any permanent findings and residual risk to the DoD.
(6) Step 4: FSO submits the STIG and MDM integration results to the DISA CIAE for review/approval of the STIG and the mobile device. Upon CIAE approval and release of the vendor STIG, the device is placed in a central repository for approved mobile devices.
(7) Step 5: The MDM Tier III support team updates the MDM to reflect the approved device and/or operating system. Approved product is placed on the approved list.

b. Commercial-Off-The-Shelf (COTS) Mobile Applications: All mobile applications on Government Furnished Equipment (GFE) CMD's will be distributed and updated from a DoD App Store. The process workflow outlined in Figure 3.2 outlines the process to be followed for the development, testing, certification, and placement of COTS mobile applications in the Mobile Apps Store. All Apps for potential inclusion in the Enterprise MAS have previously gone through the Mobility PMO's assessment/need determination process.

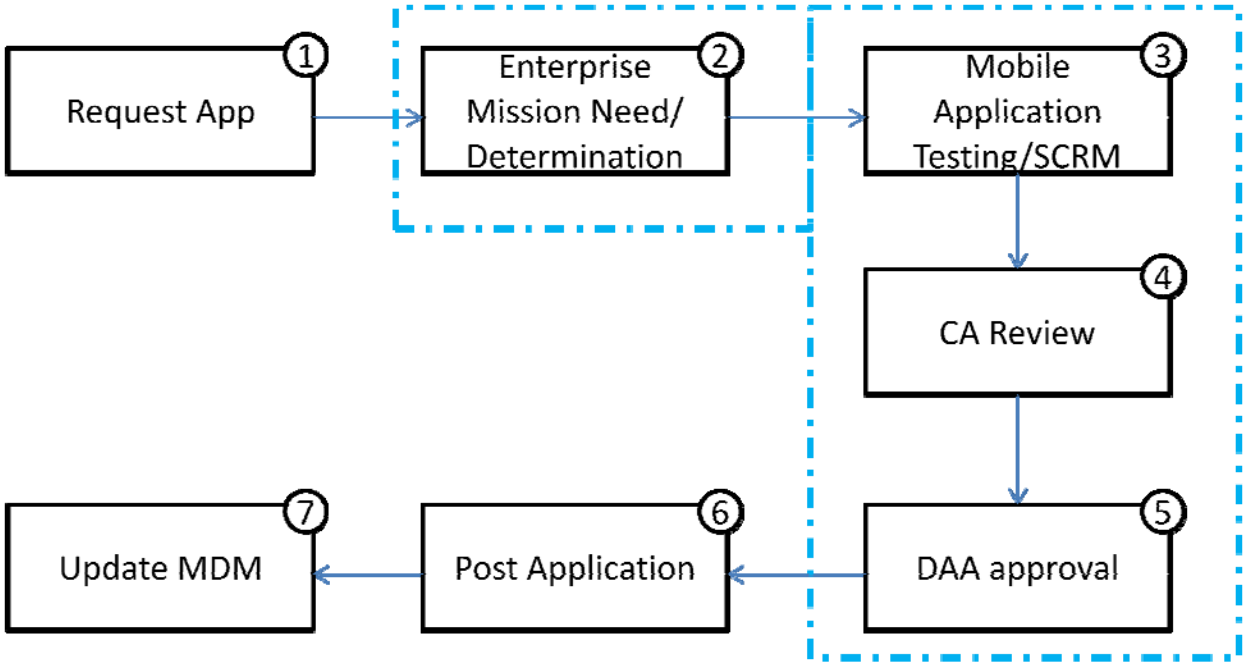

Figure 3.2 COTS Mobile Applications Vetting Process

(1) Step 1: The DoD Sponsor submits a request for a mobile application to the DISA Mobility PMO.

(2) Step 2: Mission Need Determination, is provided by the PMO for Mobility to the DoD Sponsor.

(3) Step 3: The DoD Sponsor conducts a Supply Chain Risk Assessment. The results from the Supply Chain Risk Assessment are reported to the DoD Sponsor's DAA. In parallel, the Mobile Application SRG is provided to the designated testing entity. The testing entity will determine the level of testing required, based on the Mobile Application SRG, and will utilize the appropriate security tools to evaluate the mobile application. For C2 mobile applications the Joint Interoperability Test Command (JITC) will conduct testing and certify the mobile application for interoperability. For Change Requests (CR), it is not necessary to conduct the SCRM assessment.

(4) Step 4: The CR (when applicable), Supply Chain Risk Assessment, SRG compliance validation results, and any other mobile application supporting documents are provided to the DoD Sponsor CA for review and development of a risk recommendation to the DoD Sponsor's DAA.

(5) Step 5: The DAA reviews the risk recommendation and makes an approval decision.
(6) Step 6: Upon DAA approval the mobile application is placed in the Enterprise Mobile Apps Store.
(7) Step 7: The MDM is updated to include the approved App. The list of Apps that can be accessed by each account is also updated. Users are notified of the application's availability in the Enterprise MAS.

c. Government-Off-The-Shelf (GOTS)/Open Source Mobile Applications Process: The process workflow outlined in Figure 3.3 outlines the process to be followed for the development, testing, security assessment, approval, certification, accreditation, and placement of GOTS mobile applications in the Mobile Apps Store. The testing, security assessment, approval, certification, and accreditation of open source applications/source code will follow the same procedures as those outlined for the development of GOTS mobile applications. All Apps for potential inclusion in the Enterprise MAS have previously gone through the Mobility PMO's assessment/need determination process.

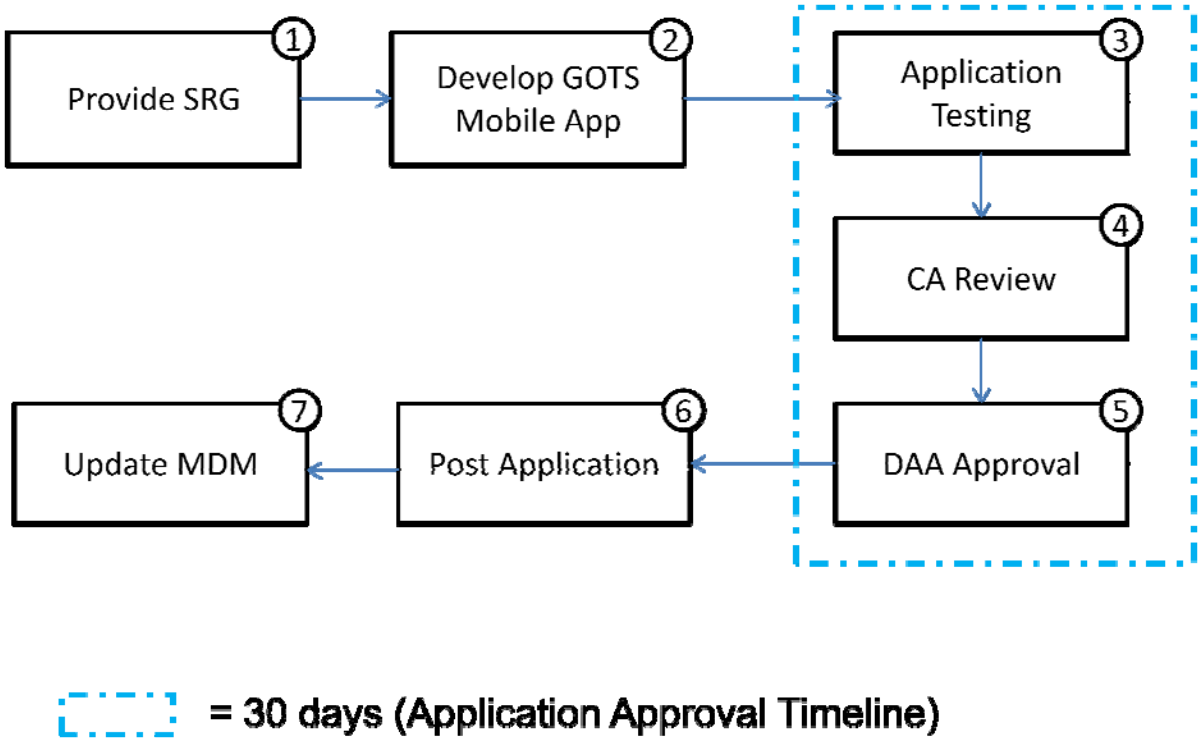

Figure 3.3 GOTS/Open Source Mobile Applications Process

(1) Step 1: DISA provides SRG compliance criteria to the DoD Sponsor.
(2) Step 2: For GOTS, the DoD Sponsor develops mobile application and test procedures based on the SRG.
(3) Step 3: The DoD Sponsor will perform compliance validation testing in accordance with the SRG. The DoD Sponsor will submit the results of SRG testing, the CR (if applicable) and all other GOTS mobile application supporting documents to the DoD Sponsor Certifying Authority (CA).
(4) Step 4: The DoD Sponsor CA performs a review of the SRG compliance validation testing, directs additional tests as necessary, and provides a risk recommendation to the DAA.
(5) Step 5: The DAA reviews the risk recommendation and makes an approval decision.
(6) Step 6: Upon approval the mobile application is placed in the Mobile Apps Store.
(7) Step 7: The MDM is updated to include the approved App. The list of Apps that can be accessed by each account is also updated. Users are notified of the application's availability in the MAS.

Appendix A - Acronym List

APL – Approved Products List
APLITS - Approved Products List Integrated Tracking System
App- Mobile Application
ATO - Authorization to Operate
C&A – Certification and Accreditation
C2 – Command and Control
CA – Certifying Authority
CCB - Configuration Control Board
CC/S/A - Combatant Commands, Services, Agencies
CIAE - Chief Information Assurance Executive
CMD- Commercial Mobile Device
COTS – Commercial-Off-The-Shelf
CTO – Chief Technology Office
DAA – Designated Approving Authority
DCC- DISA Command Center
DISN - Defense Information System Network
DoD CIO – Department of Defense Chief Information Office
FSO – Field Security Operations
GFE - Government Furnished Equipment
GIG - Global Information Grid
GO - GIG Operations
GOTS – Government-Off-The-Shelf
IA – Information Assurance
IO – Interoperability
ITSM - Information Technology Service Management
JITC – Joint Interoperability Test Command
MAS - Mobile App Store
MDM – Mobile Device Management
NETOPS – Network Operations
NS – Network Services
OPS - Operations
PKE – Public Key Infrastructure (PKI) Enabling
PKI – Public Key Infrastructure
PMO - Program Management Office
QoS – Quality of Service
SLA – Service Level Agreement
SRG - Security Requirements Guides
STIGs - Security Technical Implementation Guides
UC - Unified Capabilities
UCR – Unified Capabilities Requirement
VOIP - Voice over Internet Protocol

Appendix B – Definitions

Authorization to Operate (ATO) - Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years.

Certifying Authority (CA) - The senior official having the authority and responsibility for the certification of ISs governed by a DoD Component IA program.

Designated Approving Authority (DAA) - The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

DoD Sponsor - DoD program office that is creating or would like a specific Mobile Application approved for use.

GOTS – solutions developed by the US Government, where parts of the source code for the entire solution may not be available.

Enterprise Mobile Apps Store (MAS) - An online store for downloading applications and updates for use on commercial mobile devices.

Commercial Mobile Devices (CMDs) - Includes smartphones, tablets.

Mission Need/Determination – The Mobility PMO's assessment according to mobile application priority and additional information about a mobile application.

Mobile Device Management (MDM) - An application that gives IT administrators a way to troubleshoot and manage employee mobile devices remotely. Mobile device management software typically allows distribution of applications, data and configuration settings and patches for devices such as tablets, mobile phones, smartphones, and other mobile computing devices.

Mobile Products - Includes commercial mobile devices, operating systems, applications, and the mobile supporting infrastructure.

Mobile support infrastructure - Includes the MDM, MAS, and mVPN

mVPN (Mobile VPN) - Provides mobile devices with access to network resources and software applications on their home network, when they connect via other wireless or wired networks.

Open Source - solution not developed by the US Government where all source code is available.

Service Certifying Authority (CA) - The approving authority for the DoD sponsor for COTS/GOTS mobile applications.

SRG Compliance Validation - a process which includes manual and/or automated activities to validate that a product 1) inherently meets the requirement, 2) can be configured to meet the requirement, or 3) does not, at the current version, meet the requirement.

Supply Chain Risk Assessment - Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including malware, malicious processes, and counterfeits. Assessments can include static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by the DISA Focal Point. The authority to conduct Supply Chain Risk Management (SCRM) is in accordance with guidance provided in CNSSD 505 and DoD Instruction (DoDI) 5200.44.

Tier 1 Support - Basic customer service (i.e., open tickets, password resets, etc.).

Tier 2 Support - Optional service at an additional cost (i.e., application support, tech support, etc.).

Tier 3 Support - Optional services (i.e., external support, application developer support, etc.).