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

CHIEF INFORMATION OFFICER

FEB 15 2013

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
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: Department of Defense Commercial Mobile Device Implementation Plan

References: See Attachment 3

This memorandum provides a phased Commercial Mobile Device (CMD) Implementation Plan that promotes the development and use of mobile non-tactical applications within the Department of Defense (DoD) enterprise. The Implementation Plan updates the DoD Mobile Device Strategy, Reference (a), to permit secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products. The Implementation Plan is contingent on available funding and will be followed by a DoD Instruction with additional guidance on the use of wireless voice, video, and data capabilities.

The Defense Information Systems Agency, with oversight from the DoD Chief Information Officer (CIO), is leading the effort to create an enterprise solution to support Controlled Unclassified Information mobility requirements that will leverage commercial carrier infrastructure and provide entry points for classified services. A series of operational pilots from across the DoD Components will allow DoD to incorporate lessons learned, ensure interoperability, refine Mobile Device Management requirements, influence commercial standards, and create operational efficiencies for DoD enterprise mobile users. The point of contact for the DoD CIO is Mr. Mark Norton at: mark.norton@osd.mil, (571) 372-4941.

Teresa M. Takai

Attachments:
1. DoD CMD Implementation Plan
2. Defense Information Systems Agency's CMD Implementation Plan Phased Timeline
3. References
4. Glossary

ATTACHMENT 1

DoD COMMERCIAL MOBILE DEVICE IMPLEMENTATION PLAN

1. INTRODUCTION

This memorandum provides a phased CMD Implementation Plan that promotes the development and use of mobile non-tactical applications within the DoD enterprise. The Chairman of the Joint Chiefs of Staff's Capstone Concept for Joint Operations: Joint Force 2020, Reference (b), recognizes mobile technology as a key capability enabler for joint force combat operations. The application of mobile technology into globally integrated operations, the integration of secure and non-secure communications, and the development of portable, cloud-enabled command and control capability will dramatically increase the number of people able to collaborate and share information rapidly. Secure commercial mobile applications are increasingly viewed as essential to innovations and improved mission effectiveness across a wide range of DoD mission areas.

As a result of a JROC Capability Gap Assessment, OSD guidance, and strong end user demand for secure classified and unclassified mobile solutions, DoD is orchestrating an effort to provide wireless network services infrastructure, approved devices, applications management, and policies to protect and secure the mobile DoD information ecosystem. The Implementation Plan updates the DoD Mobile Device Strategy, Reference (a), to establish wireless voice, video, and data capabilities in accordance with DoD Instruction 8100.04, Reference (c), by October 2013. The 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.

Under the auspices of the DoD CIO Executive Board, the DoD CIO is pursuing a phased approach to mobility solutions leading to improved unclassified and classified mobile capabilities. A series of Component pilots will allow DoD to incorporate lessons learned, ensure interoperability, refine Mobile Device Management (MDM) requirements, influence commercial standards, and create cost and operational efficiencies for DoD enterprise mobile users. The Defense Information Systems Agency (DISA), with oversight from the DoD CIO, is creating an enterprise solution to support Controlled Unclassified Information (CUI) mobility requirements that will leverage commercial carrier infrastructure and provide entry points for the classified solution.

As end user dependence on mobile devices rises, enterprise management implemented via an MDM becomes necessary to ensure secure mobile device operation and maintenance in a cost-efficient manner. The MDM provides the ability to enforce policy for end user devices at application and user levels by instituting end user permissions for approved functions on the mobile device. MDM also supports malware detection, over-the-air (OTA) electronic software distribution of applications, remote data-wipe capabilities, remote device configuration management, and asset/property management capabilities that protect against key and data compromise. These capabilities ensure the security of the entire user community is not compromised by an improperly configured or operated device. A unified MDM architecture

secures, monitors, manages, and supports accredited mobile devices across a range of DoD environments.

Mobile applications are a critical enabler for service delivery and will permit new opportunities to improve mission effectiveness. This plan establishes an enterprise Mobile Application Store (MAS) capability that operates in conjunction with the MDM system. The MAS can deliver, update, and delete applications on mobile devices without the end user having to return the device for service. The objective of an enterprise MAS is to optimize the functionality and distribution of mobile applications to mobile devices while minimizing replication, cost, and downtime.

2. VISION

The DoD CMD Implementation Plan executes the goals of the Mobile Device Strategy, Reference (a), by establishing a framework to advance and evolve the DoD Information Enterprise infrastructure to support mobile devices, institute mobile device policies, and promote the development and use of mobile applications for DoD. The goal of the implementation plan is to provide a cost management process that permits mobility solutions across DoD and not to implement a specific mobile technology.

This plan defines the high-level DoD implementation approach for providing MDM that leverages the capability and usability of CMDs while protecting DoD information. Until the development of multi-level security is a viable construct, separate MDM systems in the classified and unclassified DoD information domains will be implemented. The implementation plan provides for multiple approaches in providing MDM capability for unclassified networks, while implementing a centralized methodology for classified networks.

This plan also defines the approach for the management of mobile applications. Commercial mobile technologies enable users to rapidly support their mission requirements through the discovery, purchase, and installation of mission-capable mobile applications. However, the rapid development of mobile technology requires a corresponding set of organizational processes to provide such applications. The DoD CIO's aim is to develop an overall governance process, a centralized library, and a development framework where mobile applications can be quickly developed, purchased, certified, and distributed to users.

3. APPROACH

Implementation of the Department's mobility capabilities will be guided by a continuous process of requirements evaluation and business case analyses to determine the mission and cost effectiveness of developing an enterprise solution. The implementation approach is to provide procurement and operation of CMDs via DISA, DoD Components, and the General Services Administration (GSA). A key objective is for DISA to establish a Program Office for procurement and operation of enterprise MDM capabilities and Mobility Services by Fiscal Year 2014. An integration of multiple approaches is required to implement and deploy solutions swiftly, satisfy the wide number of different DoD applications, permit a competitive acquisition

environment, enable interoperability among mobility services, and accelerate the adoption of new technologies.

DoD will establish a governance process to develop and adjudicate the standards, policies, and processes needed to effectively and efficiently manage mobile applications for the enterprise. The management process will take into account application development internal and external to DoD and leverage work completed by other Federal agencies. Mobile applications may be acquired and managed by each Component, as a service provided by GSA, and/or as an enterprise-level service managed by the DISA, as appropriate.

3.1 Governance

DoD CIO will make the final decision on enterprise mobility solutions with input from Components to ensure that they meet mission requirements and achieve best value for the Department. Under direction from the DoD CIO Executive Board, Components/Services/Agencies (C/S/A) will participate in the Commercial Mobile Device Working Group (CMDWG). The CMDWG will review and approve standards, policies, and processes for the management of mobility solutions and mobile applications on an ad-hoc basis.

Functions of the CMDWG related to cost management include:

- Develop CMD and MDM solution requirements in accordance with Reference (d) and from lessons learned as a result of pilots and consolidated DoD Components, Federal agencies, and National Security Agency (NSA) mobility implementations.
- Assess Business Case Analyses (BCA) and recommend standards, policies, and processes for the development and management of mobility solutions.
- Assess semiannual audits for comparison of mobility service approaches and recommend metrics to aid decisions on optimal management of implementation options, examples may include:
    - Evaluate inventory annually and identify: Commercial Carrier, User, Plan(s), Device (Manufacturer, Model, Operating System (OS), Electronic Serial Number (ESN) per device)
    - Compute Average Cost Per Unit (ACPU) where unit is a CMD
    - Identify Cost Per Megabyte (MB) Equivalent (includes data, voice, text)
    - Identify MB Equivalent Usage and Growth
    - Identify savings and cost avoidance compared to prior year
    - Identify overage charges and appropriate action plan
    - Identify under-utilized or zero usage devices and appropriate action plan

Functions of the CMDWG related to mobile application management include:

- Develop CMD application development requirements in accordance with Reference (d) and from lessons learned as a result of pilots and consolidated DoD Components, Federal agencies, and NSA mobility implementations.

- Establish certification and accreditation (C&A) requirements for mobile applications and ensure reciprocity across DoD Components and Federal agencies.
- Establish the authority approval process for mobile applications.
- Develop enterprise-wide, C/S/A, and single-purchase licensing procedures for mobile applications.
- Define appropriate data formats and uses of data for mobile applications (e.g., data aggregation, geo-location, machine readable policies, etc.).

3.2 Centralized Enterprise Implementation

DISA shall establish a DoD Mobility Program Management Office (PMO) that will provide guidelines for secure classified and unclassified mobile communications capabilities to the DoD on a global basis. Provision of these capabilities will be accomplished through the implementation of a mobility solution, either at the DoD or Component level, with enterprise-level mobile communications services, which will provide a Department-wide foundation for interoperability, security, access to information, and reliable service to the DoD Components.

Cognizant of the Secretary's Information Technology Efficiencies initiative, DoD will use an evolutionary acquisition approach to deliver unclassified and classified mobility capabilities to the DoD enterprise in a manner that significantly reduces cost, eliminates duplication, and promotes economies of scale. DISA will deliver capabilities in increments over a three-phase approach. The first phase of each capability implements three test spirals to refine requirements, engineering design, security, and operational concepts based on evaluations before entrance into the next spiral. The spiral approach shall support Components with migration to the enterprise solution after validating the architecture and demonstrating cost benefits. The following sections describe the unclassified and classified CMD capabilities of the centralized enterprise implementation.

An enterprise-level service capability for unclassified information processing will be accomplished by an MDM system with an enterprise MAS. The MDM system itself will be a decentralized capability hosted at several DISA Defense Enterprise Computing Centers (DECC) and/or C/S/As based on business case. For the DoD Components, the MDM system is accessed via a web portal using administrator profiles to perform policy management and technical and service provisioning for its mobile device subscribers.

By providing a library for the development, testing, and maintenance of mobile applications, cost reduction advantages can be obtained. The application library will permit code hosting, software development and assurance tools, application testing, version management control, and C&A support of mobile applications. Completed and approved mobile applications will be able to be downloaded on demand from enterprise and/or DoD Component MASs. The process will ensure all approved public and commercially available applications can be incorporated for DoD use. Utilization of application provisioning as a service from GSA will be feasible once DoD Application Governance and security requirements have been met.

The mobile application development framework will be freely available to developers and be based on commercial software development kits. The development framework will provide the

tools and test environments needed to test mobile applications in an operationally relevant environment. The operation of this framework will also include processes for application development and testing external to DoD as well as externally developed applications tested with tools internal to DoD.

A streamlined mobile application certification process is required to quickly review and certify a mobile application for operational use. This includes applications developed externally to DoD and virtual environments that represent DoD networks. The certification process will allow for the assessment of the mobile application from a security and quality perspective. This concept includes the formation of shared agreements between DoD Components. These shared agreements will outline how mobile applications will be certified so reciprocity can be established, enabling mobile applications to be certified only once.

3.3 DoD Components Implementations

A DoD Component level MDM service is an installed, supported, and managed MDM and/or MAS system that supports the DoD Component's mobile users. A DoD Component instantiated MDM and/or MAS service must meet the DoD Component's validated requirements. The DoD Component may instantiate both an MDM and MAS system for initial operational uses but must integrate their efforts into the DoD enterprise capability in accordance with a convergence plan. Additionally, network management information for instantiated MDM/MAS system(s) must be reported to DoD-level network management systems per current USCYBERCOM requirements. The DoD Component installed MDM/MAS system(s) must meet the appropriate DoD-level security requirements.

Lessons learned from Component implementations will inform development, operation, and management of credential management, common infrastructure, and mobile application development. Components will gather requirements, identify mobility pilot projects, and participate in specific pilots to guide DoD program decisions.

Component mobility pilots and initial operational uses, such as those identified in Table 1, will be evaluated to determine the impacts of proposed technologies to DoD mobility services. Systems engineering trade studies, architecture development, and cost/benefit analyses shall be made available to help guide acquisition decisions across the DoD community.

Unclassified CMD Capability	Classified CMD Capability
• Army App Store (USA) • Connecting Soldiers to Digital Apps (CSDA) (USA) • Digital Sea Bag (USN) • Warfighter's Edge (Wedge) (USAF) • Electronic Flight Bags (USAF) • ONE Mobile Application (USNORTHCOM) • mCARE Initiative (USA/TATRC) • 92Y Instructor (USA/TRADOC) • Fixed Wireless at a Distance (DARPA)	• 4G/LTE Sea Trial (USN) • SECRET BlackBerry (USSOCOM) • Trusted Handheld (USMC) • Secure iPad (SiPAD) (DARPA) • Multi-Level Security (MLS) Joint Capability Technology Demonstration (JCTD) (DISA) • JO-LTE-D TACTICS JCTD (DISA) • TIPSPIRAL (NSA)

Table 1 – DoD Component Mobility Pilots

3.4 GSA Implementation

The Digital Government Strategy, Reference (e), relies heavily upon the GSA to establish and administer federal mobility services. The Digital Government Strategy directs the GSA to:

- Establish a government-wide contract vehicle for mobile devices and wireless service.
- Set up a government-wide mobile device management platform to support enhanced monitoring, management, security, and device synchronization.
- Update the dot gov domain guidance and procedures to help ensure all new digital services meet improvement guidelines and provide support to agencies.
- Expand Data.gov to include a web API catalogue that centrally aggregates web APIs posted on agency/developer pages.
- Establish a Digital Services Innovation Center to improve the government's delivery of digital services.

DoD Components may contract for mobility services from GSA once the GSA-provided MDM/MAS support meets the appropriate DoD-level security requirements. Instantiated MDM/MAS systems must report and pass network management information to DoD-level network management systems per current USCYBERCOM requirements. DoD will continue to evaluate GSA-developed MDM/MAS solutions as they become available. In addition, DoD CIO will participate in Digital Government Strategy initiatives and assist GSA with the development of mobility requirements for federal mobility services.

4. IMPLEMENTATION FRAMEWORK

Initial guidelines to manage CMD infrastructure, devices, and applications are described below. DoD policy will be developed to provide additional guidance and incorporate lessons learned from initial enterprise mobile implementations by March 2013.

4.1 Cost Management

4.1.1 Mobile solutions will be selected to meet mission requirements and achieve best value for the Department.

4.1.2 The DoD CIO will conduct a semiannual audit that determines the total cost of mobility implementation, operation, and management.

4.2 Infrastructure

4.2.1 Acquisition contracts for CMD carrier services (e.g., mobile voice and data via cellular) shall be consolidated, to the greatest extent practical, and Department- and government-wide contracts shall be preferred to promote efficient use of government resources, in accordance with the Digital Government Strategy, Reference (e).

4.2.2 CMD carrier service accounts and usage shall be managed and monitored using a Telecommunications Expense Management (TEM) system that regulates underutilized and over-subscribed accounts, in accordance with Reference (e).

4.2.3 MDM services for control and audit of CMDs shall be established and managed at the DoD enterprise level to optimize operation and maintenance, ensure security, and support CMD synchronization. DoD enterprise MDM services shall maintain or improve upon the quality of service of Component MDM services.

4.2.4 Commercial devices and solutions and accreditable cloud solutions shall be considered, to the greatest extent possible, to reduce costs and DoD ownership and management of infrastructure.

4.3 Devices

4.3.1 A multi-vendor mobile operating system environment for CMDs shall be supported to enable a device-agnostic procurement approach.

4.3.2 Multiple form factors of CMDs will be supported and encouraged in order to meet the various operational use case scenarios.

4.4 Mobile Applications

4.4.1 A storage and distribution facility with federated management shall be established for mobile applications. Mobile applications shall be certified via an approved governance process.

4.4.2 A common mobile application development framework shall be established to enable interoperability across OSs, in accordance with Reference (d). The framework shall leverage commercial capabilities, drive the use of standards, ensure compliance with security requirements, and facilitate consistency among core functions.

4.5 Information Assurance

4.5.1 The CMD security approval process shall be streamlined with the objective of a 90-day approval cycle for mobile devices and operating systems. The approval process for mobile devices will work towards a device-agnostic approach based on SRGs produced by DISA FSO. Vendor developed STIGs will be based on the appropriate SRG and submitted to DISA FSO for validation.

4.5.2 Established DoD Information Assurance Certification and Accreditation Process (DIACAP) certified connection methods shall provide identity attributes for authenticated credentials to make secure, real-time, and reliable access decisions.

4.5.3 The DoD mobility capability shall integrate into established cyber-situational awareness and Computer Network Defense (CND).

4.5.4 Remote scanning and continuous monitoring shall be employed by MDM systems to enforce policy compliance for configuration of applications and OSs thereby minimizing the need for user-based enforcement.

4.5.5 Current guidance on information spillage at the Department and Component levels applies to mobile devices.

4.5.6 CMD application development initiatives and pilot demonstrations shall conform to established security guidelines and obtain approval before connecting to a DoD network, in accordance with References (d) and (f).

4.5.7 The processing of unclassified information on commercial mobile infrastructure, devices, and applications shall be performed in accordance with References (d), (f), (g), and (h); and:

4.5.7.1 CUI shall be protected via approved processes, which may include Public Key Infrastructure (PKI) credentials (e.g., Common Access Card), in accordance with DoDI 8520.02, Reference (i).

4.5.7.2 User Based Enforcement (UBE) controlled security settings are permitted with an established training and audit program to minimize overall risk when technical controls are infeasible to implement, on a case-by-case basis as determined by the Designated Accrediting Authority (DAA).

4.5.8 The processing of classified information on commercial mobile infrastructure, devices, and applications shall be performed in accordance with References (g) and (h) and National Security Directive (NSD)-42, Reference (j); and:

4.5.8.1 A minimum of two independent layers of Suite B encryption shall be used to protect all classified data in transit, in accordance with Reference (k).

4.5.8.2 CMD architectures and implementations for National Security Systems containing or processing classified information shall follow NSA standards.

4.5.8.3 Voice communications shall be protected via Secure Voice over Internet Protocol (SVoIP). Gateways shall be established to permit interoperability with legacy voice communications systems (e.g., Public Switched Telephone Network (PSTN)).

4.5.8.4 Secret Internet Protocol Router Network (SIPRNet) hardware tokens shall be used to provide trusted user identification and authentication to SIPRNet resources.

4.6 Training. DoD Components shall ensure that all DoD mobile users are aware of their responsibilities and trained in the proper configuration and use of CMDs.

4.7 Other. Potential use cases and implementations of personally owned, personally used devices for connections to DoD networks will be studied, in accordance with Reference (e).

5. RESPONSIBILITIES

The key officials who shall implement this implementation plan and the overarching duties and obligations of each are described below.

5.1 DoD CIO will:

5.1.1 In coordination with the Director, DISA, and Component CIOs, make the final decision on enterprise mobile solutions to ensure that they meet mission requirements and achieve best value for the Department.

5.1.2 In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), define the appropriate consolidated acquisition approach for the procurement of CMD carrier services (e.g., cellular).

5.1.3 In coordination with the USD(AT&L), define the appropriate methods to measure the total lifecycle cost of mobility services. Review and assess semiannual audits to determine optimal management of mobility service solutions.

5.1.4 Define within 120 days UBE guidelines for sensitive unclassified information processing.

5.1.5 Develop and publish policy and guidance within 120 days for a controlled-access MAS solution to meet CMD objectives/thresholds (e.g., ensure mobile applications are obtained from trusted sources using approved authentication methods, such as digital signatures).

5.1.6 Assess options within 120 days for streamlining the CMD security approval process.

5.1.7 In coordination with the DoD PKI PMO and the NSA, develop and publish guidance to ensure that PKI implementations for CMDs support approved PKI credentials (e.g., Common Access Card).

5.1.8 Develop and publish guidance for implementations of personally owned, personally used devices (e.g., virtualization of mobile OSs) following promulgation of government-wide guidance, when appropriate.

5.1.9 Under the auspices of the DoD CIO Executive Board, oversee the CMDWG to review and approve standards, policies, and processes for the management of mobility solutions.

5.2 Director, DISA will:

5.2.1 Establish within 120 days a DoD Mobility PMO that will provide guidance for secure classified and unclassified mobile communications capabilities to the DoD on a global basis.

5.2.2 Develop within 90 days a Business Case Analysis (BCA), outlining all costs, reimbursables, and timelines for full deployment of all mobile capabilities.

5.2.3 In coordination with the NSA/Central Security Service (CSS), develop and publish guidance for mobile and wireless security architectures.

5.2.4 Develop and maintain an enterprise MDM service platform.

5.2.5 Define and publish a methodology for connecting CMDs via approved commercial carrier services, in accordance with Reference (g).

5.2.6 Establish and maintain a qualified product list of CMDs that may be connected to DoD networks in accordance with DoD policy.

5.2.7 Develop and publish within 150 days guidance for application management and certification processes.

5.2.8 Develop a controlled-access, tiered (e.g., user-end, enterprise, database) MAS to serve as a central repository for certified mobile applications.

5.2.9 Publish within 120 days guidance for development of mobile applications to promote interoperability across CMD platforms, extensibility, and code reuse (e.g., use platform agnostic programming languages, such as javascript, to the greatest extent possible; standardize security functions; recommend common metadata tagging standards; and base development frameworks on Software Development Kits/Application Program Interfaces).

5.2.10 Modify the security approval process for mobile devices, OSs, and applications to ensure that DoD will have access to the latest mobile technologies in a timely manner by maximizing vendor participation.

5.2.10.1 DISA Field Security Office (FSO) will publish Security Requirements Guides (SRG) as a core set of relevant security controls based upon applicable NIST guidance.

5.2.10.2 DISA FSO will provide guidelines for vendors to publish Security Technical Implementation Guides (STIG) to meet SRG requirements for particular mobile products, perform self-certification of their products, and submit the STIG and self-certification documentation for review.

5.2.10.3 DISA FSO will validate the vendor's STIG and self-certification documentation and will submit the package to the DISA Chief Information Assurance Executive (CIAE) for approval.

5.2.10.4 Approved mobile devices, OSs, and applications will be placed on the DoD CIO Unified Capabilities Approved Products List (UCAPL) within 3 weeks, in accordance with Reference (c).

5.2.10.5 Additional interoperability testing is required when solutions implement Assured Service Features (ASF).

5.2.11 In coordination with the DoD PKI PMO and NSA, recommend options within 180 days for the development of integrated PKI credentials for CMDs (e.g., microSD Hardware Security Module (HSM)).

5.3 USD(AT&L) will assist the DoD CIO and the CMDWG in crafting an approach(es) for the acquisition of services to support the goal of acquiring cost effective secure classified and protected unclassified mobile solutions for the Department.

5.4 Director, NSA, under the authority, direction, and control of the Under Secretary of Defense (Intelligence), will:

5.4.1 Review and approve all standards, techniques, systems, and equipment related to the security of national security systems.

5.4.2 Define within 120 days processes under the NSA Commercial Solutions for Classified (CSfC) Program by which mobility solutions may be implemented based on commercial technologies that will protect National Security System information.

5.4.3 In coordination with the DoD PKI PMO and DISA, recommend options within 180 days for the development of integrated PKI credentials for CMDs (e.g., microSD HSM).

5.4.4 Provide within 120 days updated guidance on CMD use with respect to TEMPEST policies.

5.4.5 Implement a capability to assess the risks and vulnerabilities associated with CMD technologies that are responsive to DoD requirements including, for example, CMD encryption and authentication protocols.

5.4.6 Develop and disseminate threat information regarding the capabilities and intentions of adversaries to exploit CMD technologies used by the DoD Components.

5.4.7 Provide IA guidance for CMD technologies, including protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.5 DoD Component CIOs will:

5.5.1 Conduct and publish a semiannual audit that determines the total cost of mobility implementation, operation, and management.

5.5.2 Use the enterprise MDM service platform in accordance with a convergence plan and POM Mobility requirements including devices and data plans starting in FY15 and beyond.

5.5.3 Implement mobile and wireless security architectures in accordance with DISA and NSA/CSS guidelines and standards.

5.5.4 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 DoD CIO and make the applications available to the MAS. Develop application management guidelines, certification processes, and sustainment capability consistent with DISA guidance. Ensure that CMD application development and pilot demonstrations conform to established security guidelines and have been reviewed and approved by cognizant authorities before they are connected to DoD networks.

5.5.5 Identify within 120 days existing CMD application pilot activities and report the information to the DoD CIO, in accordance with Reference (f).

5.5.6 Identify subject matter experts and C/S/A leads and coordinate with respective MDM, MAS, Multi-Carrier Entry Point (MCEP), and other related mobile working groups.

6. PROCEDURES

The sequence of actions to be taken and instructions to be followed to accomplish the enterprise implementation are described below and in DISA's Commercial Mobile Device Implementation Plan Phased Timeline, Attachment 2.

6.1 Unclassified CMD Capability

Several implementation options for the unclassified MDM capability will be assessed and qualified during the phased capability development. Contingent on the availability of FY 13-14 funding, a consolidated implementation that incorporates DISA MDM and MAS infrastructure will be established for the DoD enterprise. The consolidated DoD enterprise implementation will be architected to allow users of commercial carrier-based implementations to procure MDM services via GSA contracts and to allow decentralized implementations among the Components that permit local MDM with access to centralized credential and application management enterprise resources. The phased timeline of DISA's enterprise implementation is described in Attachment 2.

6.2 Classified CMD Capability

NSA has established the CSfC process to enable use of commercial products in layered solutions to protect classified National Security Systems data. The process satisfies customers' urgent requirements to communicate securely with interoperable products based on commercial standards in a solution that can be fielded in months. The architecture, security guidelines, and standards required for implementing enterprise mobile solutions with commercial products are published in the Mobility Capability Package (MCP), Reference (k). The latest version of this document is posted on http://www.nsa.gov.

Enterprise mobility is supported by the use of commercial cellular and wireless devices to access classified data and voice services while minimizing the risk when interconnecting to existing enterprise services. The commercial carriers and other unclassified access networks provide the controlled connectivity between end users and the Government enterprise. Centralized management and control of secure classified mobile communications services and devices will be provided. Classified voice and data communications up to classification level of Top Secret (TS) will be supported. Goals for the classified CMD capability shall be consistent with the subset of the Senior Leader Secure Communications Modernization (SLSCM) Implementation Plan, Reference (l). The phased timeline for DISA's enterprise implementation is described in Attachment 2.

6.3 Future Capability

The following capabilities will be studied and explored as future enhancements to the DoD mobility solution.

6.3.1 Joint Information Environment

Mobility solutions will leverage the enterprise capabilities within the Joint Information Environment (JIE) and will be codified in the solution architectures based on the DoD Information Enterprise Architecture (IEA), Reference (m).

6.3.2 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) or personally owned devices used for enterprise business purposes is an emerging trend throughout the IT industry. This new construct presents many compelling benefits to organizations and users and is a long term objective. Despite the benefits, existing DoD policies, operational constructs, and security vulnerabilities currently prevent the adoption of devices that are unapproved and procured outside of official government acquisition. DISA and various DoD Components are currently examining the use of virtual desktop infrastructure (VDI) as a possible technology approach to bridge the security gap for BYOD. Another approach is the development of “hardened” devices capable of a secure boot of trust and isolated hypervisors based on the Trusted Platform Module (TPM). TPM is both the name of a published specification detailing a secure crypto-processor that can store cryptographic keys, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device". Several mobile device original equipment manufacturers are moving toward producing CMDs with the capability to securely support both an enterprise and a personal capability on the same device. As the technology matures and is proven to meet DoD security requirements for the mobility environment, DoD CIO will monitor and generate the necessary DoD implementation policies to support BYOD. In conjunction with the Digital Government Strategy, DoD will continue to evaluate BYOD options.

6.3.3 First Responder Network

DoD partners with other federal and civil authorities when responding to significant local, regional, and national emergencies. As the technology available to emergency responders matures via the First Responder Network Authority (FirstNet) Radio Access Network (RAN), DoD must assist in establishing security and interoperability standards. The ability to leverage CMDs to augment, enhance, or replace existing communication capabilities is considered a total force (e.g., DoD, Federal, and Civil) enabler that will empower a new generation of digital collaboration technology. Mobile devices with reach-back to network-based services will allow distributed commanders and staffs to collaborate as though co-located. Developing networks that can simultaneously integrate DoD and public safety networks will widen the circle of actors who can support a given operation, allowing diverse stakeholders to contribute insights and expertise in real time. Future mission command will thus be highly collaborative as seniors and subordinates join in a circle of feedback, initiative, adaptation, and mission effectiveness.

6.3.4 Improved Security Features

Advances in technology may permit additional security features to strengthen the overall information assurance posture of DoD networks. Technologies to be examined include, but are not limited to, encrypting all voice traffic via Voice over Secure Internet Protocol (VoSIP), implementing 1024-bit encryption, and biometric techniques.

ATTACHMENT 2

DISA'S COMMERCIAL MOBILE DEVICE IMPLEMENTATION PLAN PHASED TIMELINE

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

FEB 4 2013

IN REPLY REFER TO Director (D)

MEMORANDUM FOR DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

SUBJECT: DISA's Commercial Mobile Device Implementation Plan Phased Timeline

Reference: (a) Department of Defense Commercial Mobile Device Strategy

1. As the lead Agency for implementation of the DoD CIO Mobile Device Strategy (ref a), we are developing enterprise-level secure classified and protected unclassified mobile solutions that leverage commercial off-the-shelf products.

2. The enclosed DISA Commercial Mobile Device Implementation Plan Phase Timeline provides an overview of our phased approach and a timeline of deliverables. The timeline will support DoD planning to leverage the availability of enterprise-level capabilities.

3. My POC is Mr. John Hickey, DISA's Mobility Program Manager, (301) 225-3823 or John.J.Hickey20.civ@mail.mil.

1 Enclosure a/s

RONNIE D. HAWKINS, JR.
Lieutenant General, USAF
Director

DISA's Commercial Mobile Device Implementation Plan Phased Timeline

The phased timeline of actions and instructions that support DoD enterprise implementation of CMD capabilities are described below.

1. UNCLASSIFIED CMD CAPABILITY

Several implementation options for the unclassified MDM capability will be assessed and qualified during the phased capability development. Contingent on the availability of FY13-14 funding, a consolidated implementation that incorporates DISA MDM and MAS infrastructure will be established for the DoD enterprise. The consolidated DoD enterprise implementation will be architected to allow users of commercial carrier-based implementations to procure MDM services via GSA contracts and to allow decentralized implementations among the Components that permit local MDM with access to centralized credential and application management enterprise resources. DISA will conduct the implementation of MDM/MAS in three phases. Each phase builds on the previous one to provide new and/or enhanced capabilities and services. In each phase, the MDM/MAS system must meet DoD-level security requirements. The approach of each phase follows.

1.1 Phase 1, November 2012 – April 2013

Phase 1 establishes a basic multi-vendor mobility capability within DoD for assessment. Phase 1 will deploy voice and data services over a commercial wireless network and award a contract for the initial DoD enterprise MDM and MAS. Phase 1 is divided into three spirals that test reliability, user performance, and cost benefit of different vendor configurations. The objective is to establish the enterprise mobility architecture that will provide secure delivery of email, mobile applications, voice, and other data services, including initial network operations (NETOPS) and reporting capabilities. Phase 1 will include the purchase of 1,500 devices by DISA and the ability to provision additional C/S/A devices that are approved by DISA with associated mobile applications that have been vetted through the mobile application governance process identified in this implementation plan.

A series of rapid spirals will be conducted successively. The intent of the spirals is to provide the learning and expertise in deploying, operating, supporting, and upgrading services to mobile devices while maintaining the security integrity of DoD Information Systems. Spirals 1 and 2 focus on solutions for the processing of unclassified information, while Spiral 3 will also incorporate the initial instantiation of a classified capability. The baseline set of requirements will be developed during Phase 1 and subsequently vetted with the DoD Components. The key objective of Phase 1 is to develop the MDM and MAS requirements and operational processes.

Phase 1 will evaluate the performance of the centralized provisioning and management approach for unclassified service delivery. In addition, the security performance of multiple mobile OSs and applications will be reviewed to determine which will be supported and/or what additional security measures may be necessary to achieve objective performance goals.

Capabilities in Phase 1:

- Initial Mobile Device Management / Mobile Applications Store (MDM/MAS) Capability
- Develop Initial Architecture for identified capabilities
- Establish Initial Network Operations (NetOps) Reporting Approach
- Establish a Mobile Applications (Apps) Governance Process
- Deploy a up to 1,500 (DISA provided) devices
- Establish user/device support

1.2 Phase 2, April – September 2013

Phase 2's primary goal is to create a security and service delivery infrastructure to support several competitive acquisition options. Deliverables for Phase 2 include a network infrastructure to support the user community including C/S/A and a total of 5,000 devices procured through DISA and deployed to a combination of Army, Air Force, Navy, Joint Staff, and Combatant Command users. DISA will establish a NETOPS and reporting function to support the situational awareness and defense of the mobile enterprise capability. DISA will procure an enterprise MDM/MAS license to support up to 25,000 devices during this period with options in 25,000 device increments to support additional infrastructure and surge requirements in the out years depending on requirements and funding availability. The C/S/A will be responsible for procuring the approved devices required for the enterprise and the associated data plans for the devices. DISA will work with GSA and C/S/A to establish the contracts to purchase these devices with security requirement guidance. C/S/As will be responsible for Tier 1 Level 1 help desk functions as they are today with current smartphones and will have access to provisioning and help desk NETOPS capability.

Upon Phase 1 obtaining its Interim Authorization to Operate (IATO), Phase 2 will commence. During the 9-month time period of Phase 2, DISA will implement the initial Enterprise Mobility Service capability in the classified and unclassified domains and scale capability to support a large array of DoD mobile subscribers. The Enterprise Mobility Service will become a reimbursable Defense Information Systems Network (DISN) provided service. Decisions on hosting and costs will be decided after a business case is developed and courses of action are coordinated with C/S/As. The key objective of Phase 2 is the implementation of the enterprise service level capabilities to provide decentralized tier-level management for the DoD Components.

Another objective of Phase 2 is to assess the infrastructure on both unclassified and classified networks to leverage commonality and determine security and cost benefit that could be realized through a common technical approach. This integrated effort must support the Business Support Systems (BSS) and Operation Support Systems (OSS) to create unified support systems for both classified and unclassified users, once proven cost effective. The MDM OSS and its integration into enterprise-wide situational awareness and cyber defense capabilities will be evaluated in this phase and any shortcomings will be addressed prior to proceeding to Phase 3.

Capabilities in Phase 2:

- Provide capability to manage up to 5,000 DISA devices
- Develop a plan for MDM/MAS enhancements

1.3 Phase 3, October 2013 and beyond

Phase 3 is an operational capability that will be offered to the enterprise as a subscription-based service. Plans will support 100,000 devices by 2QFY14 with additional service provided as requirements and funding dictate. Management and control of unclassified mobile communications services and devices will be provided as determined by the outcomes of Phases 1 and 2. Deliverables for Phase 3 include enterprise services to support the user community including C/S/A. C/S/As will be responsible for Tier 1 Level 1 help desk functions as they are today with current smartphones. DISA will establish enterprise contracts to support the purchase of approved devices and discounted data plans using GSA and C/S/A contracts.

On a continuing basis in 18-month cycles, the Enterprise Mobility Service will be refreshed to stay synchronized with the rapid technological advances in the industry. These upgrades will be funded via received reimbursable funding. The key objective of Phase 3 is the integration of new capabilities that provide improved service and/or lower mobile subscriber cost.

Capabilities in Phase 3:

- Provide enhanced infrastructure gateway
- Provide growth capacity up to 100,000 devices in FY14
- Transition operations to subscription services
- Establish a decentralized tier 1 help desk structure
- Establish a technology refresh program

2. CLASSIFIED CMD CAPABILITY

NSA has established the CSfC process to enable use of commercial products in layered solutions to protect classified National Security Systems data. The process satisfies customers' urgent requirements to communicate securely with interoperable products based on commercial standards in a solution that can be fielded in months. The architecture, security guidelines, and standards required for implementing enterprise mobile solutions with commercial products are published in the Mobility Capability Package (MCP), Reference (k). The latest version of this document is posted on http://www.nsa.gov.

Enterprise mobility is supported by the use of commercial cellular and wireless devices to access classified data and voice services while minimizing the risk when interconnecting to existing enterprise services. The commercial carriers and other unclassified access networks provide the controlled connectivity between end users and the Government enterprise. Centralized management and control of secure classified mobile communications services and devices will be provided. Classified voice and data communications up to classification level of Top Secret (TS) will be supported. Goals for the classified CMD capability shall be consistent with the

subset of the Senior Leader Secure Communications Modernization (SLSCM) Implementation Plan, Reference (l), that applies to each phase.

A centralized enterprise service management approach for classified information processing will be accomplished via an MDM capability. The MDM system itself will be a decentralized capability hosted at several DISA DECCs. For the DoD Components, the MDM system is accessed via a web portal using administrator profiles. DISA will have access and capability to enforce DoD policy management. DISA will also be responsible for the technical and service provisioning for those agencies' classified subscribers. This responsibility includes enforcement of stricter policies as requested by each agency. Each DoD Component will have a trusted agent that will be able to perform limited functions. DISA will provide initial provisioning of the device, OTA updates, technical support, and customer support. The centralized management approach for classified is required to comply with security requirements to protect classified information.

2.1 Phase 1, November 2012 – February 2013

Phase 1 will adapt the existing MCEP to support data access to SIPRNet using commercial standards and architecture defined in NSA's MCP. Phase 1 provides an operational system based on NSA's TIPSPIRAL pilot to provide users with voice and data services. The mobility solution will establish, manage, and maintain SVoIP as an operational capability. Phase 1 will address the initial capacity, reporting, interoperability, and future scalability of the MCEP, leveraging the MCEPs and DECCs. Phase 1 will consist of several spirals that will deliver increments of capability. A Major Decision Point will be accomplished before transitioning to Phase 2 to review testing data and system performance. DISA will leverage the initial unclassified NETOPS and help desk support integrating CND functions for unclassified and classified operations to reduce overall costs.

Capabilities in Phase 1:

- Leverage the DISA Multi-Carrier Entry Point (MCEP) to establish the initial Mobility Classified Gateway (MCG) up to 500 devices
- Deliver SECRET/Voice Over Internet Protocol (S/VoIP) capability

2.2 Phase 2, March – September 2013

Phase 2 continues MCEP development for deployment to the entire DoD enterprise. Phase 2 will implement centralized management, identity certificates, integrity controls, and OTA control of secure classified mobile communications services. The key objectives of Phase 2 are to continue the transition of Secure Mobile Environment Portable Electronic Device (SME PED) users and to develop enterprise controls for classified information processing. DISA will provide a NETOPS capability that provides situational awareness and CND functions integrating with the unclassified capability.

Capabilities in Phase 2:

- Provide initial or enhance enterprise e-mail capability
- Extend Gateway access to OCONUS users and increase capacity up to 1,500 devices
- Deliver TOP SECRET/Voice Over Internet Protocol (TS/VoIP) capability

2.3 Phase 3, October 2013 and Beyond

Phase 3 is an operational capability that will be offered to the enterprise as a subscription-based service. Centralized management and control of secure classified mobile communications services and devices will be provided.

Capabilities in Phase 3:

- Transition operations to subscription service
- Initial Enterprise Classified MDM
- Initial Enterprise Classified MAS

ATTACHMENT 3

REFERENCES

(a) DoD CIO Memorandum, “Department of Defense Mobile Device Strategy,” version 2.0, June 8, 2012
(b) Chairman of the Joint Chiefs of Staff, "Capstone Concept for Joint Operations: Joint Force 2020," September 10, 2012
(c) DoD Instruction 8100.04, “DoD Unified Capabilities (UC),” November 9, 2010
(d) DoD CIO Memorandum, “DoD Commercial Mobile Device (CMD) Interim Policy,” January 17, 2012
(e) Office of Management and Budget, “Digital Government Strategy: Building a 21st Century Platform to Better Serve the American People,” May 23, 2012
(f) DoD CIO Memorandum, “Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD),” April 6, 2011
(g) 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
(h) DoD Instruction 8420.01, “Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies,” November 3, 2009
(i) DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” May 24, 2011
(j) National Security Directive (NSD)-42, “National Policy for the Security of National Security Telecommunications and Information Systems,” July 5, 1990
(k) National Security Agency, "Mobility Capability Package," as amended
(l) DoD CIO, “Senior Leader Secure Communications Modernization (SLSCM) Implementation Plan,” as drafted
(m) Department of Defense (DoD) Information Enterprise Architecture (lEA) 2.0, August 10, 2012
(n) Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," April 26, 2010

ATTACHMENT 4

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

Unless otherwise noted, these terms and their definitions are for the purposes of this memo.

ACPU	Average Cost Per Unit
ASF	Assured Service Features
BSS	Business Support Systems
C&A	Certification and Accreditation
C/S/A	Components/Services/Agencies
CIAE	Chief Information Assurance Executive
CMD	Commercial Mobile Device
CMDWG	Commercial Mobile Device Working Group
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CSfC	Commercial Solutions for Classified
CSS	Central Security Service
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
ESN	Electronic Serial Number
FSO	Field Security Office
GIG	Global Information Grid
GSA	General Services Administration
HSM	Hardware Security Module
IA	Information Assurance
IATO	Interim Authorization to Operate
JCTD	Joint Capability Technology Demonstration
JIE	Joint Information Environment
MAS	Mobile Application Store
MB	Megabyte
MCEP	Multi-Carrier Entry Point
MCP	Mobility Capability Package
MDM	Mobile Device Management
MLS	Multi-Level Security
NETOPS	Network Operations
NSA	National Security Agency

NSD	National Security Directive
OS	Operating System
OSS	Operation Support Systems
OTA	Over-the-Air
PK	Public Key
PKI	Public Key Infrastructure
PMO	Program Management Office
PSTN	Public Switched Telephone Network
RAN	Radio Access Network
SiPAD	Secure iPad
SIPRNet	Secret Internet Protocol Router Network
SLSCM	Senior Leader Secure Communications Modernization
SME PED	Secure Mobile Environment Portable Electronic Device
SOCOM	Special Operations Command
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
SVoIP	Secure Voice over Internet Protocol
TATRC	Telemedicine & Advanced Technology Research Center
TEM	Telecommunications Expense Management
TPM	Trusted Platform Module
TRADOC	Training and Doctrine Command
TS	Top Secret
UBE	User Based Enforcement
UC	Unified Capabilities
UCAPL	Unified Capabilities Approved Products List
USD(AT&L)	Under Secretary of Defense Acquisition, Technology, and Logistics
VDI	Virtual Desktop Infrastructure
VoSIP	Voice over Secure Internet Protocol
WLAN	Wireless Local Area Network

PART II. DEFINITIONS

BSS. The back-office software for billing, order management, distribution and order fulfillment, and management of the customer experience.

CMD. As defined in Reference (d), a subset of portable electronic devices (PED) as defined in DoDD 8100.02, Reference (g), 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.

MAS. The approved repository of certified software applications that a user could add to the basic functionality of a wireless device.

MDM. A process that secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers and enterprises.

Mobile Application. As defined in Reference (d), software that runs on CMDs according to permissions granted by the user upon installation and is commonly known as an "app" by the consumer industry.

OSS. The back-office software for MDM and technical provisioning of end user devices, including access control, security, and configuration management.

SRG. A compendium of DoD policies, security regulations, and best practices for securing IA or IA-enabled operating systems, networks, applications, or policies.

TEM. A proactive service that provides inventory management, monthly auditing of invoices, cost allocation, management reporting and ongoing optimization recommendations.

TEMPEST. As defined in Reference (n), a name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

UBE. The process of granting or denying specific requests for obtaining and using wireless network services under the configuration and control of the CMD user, as opposed to organization or enterprise-level configuration and control.