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

CHIEF INFORMATION OFFICER

JUN -8 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
DIRECTOR OF THE DOD FIELD ACTIVIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS

SUBJECT: Department of Defense Mobile Device Strategy

Department of Defense forces have been and continue to be increasingly mobile. Today's mobile devices potentially provide our mobile workforce with greater access to information, enhancing effectiveness and improving operational advantage. The DoD Mobile Device Strategy identifies the vision and goals for capitalizing on the full potential of mobile devices and supports the end-user services approach in the DoD Information Technology Enterprise Strategy and Roadmap. It is intended to align the progress of various mobile device pilots and initiatives across DoD under common objectives, ensuring that the warfighter benefits from such activities and aligns with efforts composing the Joint Information Environment. An implementation plan will follow, which will include further detail, as well as a communications plan to address the cultural challenges associated with mobile device deployment.

The existing Commercial Mobile Device Working Group will support follow-on strategy efforts. The point of contact is Mr. Mark Norton at email: mark.norton@osd.mil, 703-607-0711.

Teresa M. Takai

Attachments:
As stated

Unclassified

Department of Defense Mobile Device Strategy

Version 2.0

May 2012

Office of the DoD Chief Information Officer

Foreword

Computing technology is more mobile than ever. Its evolution from large mainframes to handheld mobile devices offers unprecedented opportunities to advance the operational effectiveness of the Department of Defense (DoD). Through faster access to information and computing power from any location, field units can maneuver unfamiliar environments with real-time mapping and data overlay capabilities; soldiers can identify friendly forces; engineers can take pictures of mechanical parts for immediate identification and replacement ordering; and military healthcare providers can diagnose injuries and remotely access lab results while away from hospital premises. Additionally, by enabling real-time access to important management and productivity tools (e.g., email, collaboration), warfighter support functions can be used to more quickly and responsively manage the business of the DoD.

A mobile device, for the purpose of this strategy, is a handheld computing device with a display screen that allows for user input (e.g., touch screen, keyboard). When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information given device limitations (i.e., screen size, computing power). Mobile devices provide the conveniences of conventional desktops or laptop computers in a more portable package. Popular form factors for mobile devices are smartphones and tablets.

A wireless infrastructure, as referenced in this strategy, is simply an expansion of the DoD Information Enterprise in support of mobile devices. New and existing wireless networks may be leveraged collectively to connect technologies or capabilities as needed.

The ***DoD Mobile Device Strategy*** identifies information technology (IT) goals and objectives to capitalize on the full potential of mobile devices. It focuses on improving three areas critical to mobility: wireless infrastructure, the mobile device itself, and mobile applications. It allows mobile activities across the Department to converge toward a common vision and approach. Although mobile devices are the new and popular item in today's commercial market, this strategy is not simply about embracing the newest technology – it is about keeping the DoD workforce relevant in an era when information and cyberspace play a critical role in mission success.

This strategy provides the foundation for the development of policy and an implementation plan. Successful execution relies on the cooperation and collaboration of all DoD Components and on partnerships with federal, intelligence, academia, and commercial communities. With your support, we will equip our forces with the capability to quickly access relevant information whenever and wherever needed.

DoD Chief Information Officer

Table of Contents

Foreword i
Mobility Vision 1
Goal 1: Advance and Evolve the DoD Information Enterprise Infrastructure to Support Mobile Devices 2
Objective 1: Evolve spectrum management. 2
Objective 2: Expand infrastructure to support wireless capabilities. 2
Objective 3: Establish a mobile device security architecture. 3
Goal 2: Institute Mobile Device Policies and Standards 3
Objective 1: Develop mobile device policy and standards. 3
Objective 2: Establish a mobile device management service. 4
Objective 3: Educate and train mobile device users. 4
Goal 3: Promote the Development and Use of DoD Mobile and Web-Enabled Applications 4
Objective 1: Establish a common mobile application development framework. 5
Objective 2: Institute a mobile application certification process. 5
Objective 3: Provide an enterprise mobile application environment. 5
Objective 4: "Web-enable" IT capabilities for mobile device support. 5
Implementation Considerations Based on Type of User 6
Next Steps 7

Exhibits

Exhibit 1: Goals 1
Exhibit 2: Implementation Considerations 6

Mobility Vision

A highly mobile workforce equipped with secure access to information and computing power anywhere at anytime for greater mission effectiveness.

The nature of the DoD workforce is mobile. Its mission requires the provision of forces over air, land, and sea, across foreign borders, and into adverse conditions. Civilians and military personnel regularly rotate across organizations; leadership and field units regularly travel from place to place; and a growing number of teleworkers are beginning to operate from locations other than their primary offices. The mobile workforce's ability to access information and computing power can improve information sharing, communication, and action response time for greater mission effectiveness.

Much of today's mobile society has the ability to access information and computing power due to the advent of affordable mobile devices. The rapid penetration of mobile devices into the commercial market and their projected growth demonstrate the demand for such capabilities. Their impact is widespread. Individuals leverage them to manage their everyday lives; industries employ them to improve productivity; and most recently, organizations use them to provide information in support of global situational awareness during events such as natural disasters and political conflict.

> "Worldwide mobile device sales to end users totalled 1.6 billion units in 2010. Smartphone sales to end users were up 72.1% from 2009 and accounted for 19% of total mobile communications device sales in 2010."
>
> ***Gartner, February 9, 2011***
> Gartner Press Release, Gartner Says Worldwide Mobile Device Sales to End Users Reached 1.6 Billion Units in 2010; Smartphone Sales Grew 72 Percent in 2010, http://www.gartner.com/it/page.jsp?id=1543014.

From office productivity to tactical operations, the potential for mobile devices to strengthen the DoD workforce is manifold. As such, DoD will evolve the information enterprise to capitalize on the use of mobile devices. To guide this evolution, DoD will focus on three goals (Exhibit 1).

GOAL	DESCRIPTION
1. Advance and evolve the DoD Information Enterprise infrastructure to support mobile devices	Improves wireless infrastructure to support the secure access and sharing of information via voice, video, or data by mobile devices.
2. Institute mobile device policies and standards	Establishes policies, processes, and standards to support secure mobile device usage, device-to-device interoperability, and consistent device lifecycle management.
3. Promote the development and use of DoD mobile and web-enabled applications	Provides the processes and tools to enable consistent development, testing, and distribution of DoD-approved mobile applications for faster deployment to the user. Establishes policy, processes, and mechanisms for appropriately web-enabling critical DoD IT systems and functions for mobile devices.

Exhibit 1: Goals

Goal 1: Advance and Evolve the DoD Information Enterprise Infrastructure to Support Mobile Devices

> "The increasing use of social media, smartphones, and tablet computers has made information sharing an expectation. Our challenge today is ensuring our networks can securely support the information demands of our users – users who require access to information anywhere and anytime across the DoD Information Enterprise, allowing them to make informed decisions in the execution of their missions."
>
> ***Teri Takai, DoD CIO***

A wireless infrastructure untethers the user from the confines of a desk. It enables the user—equipped with a mobile device—to maintain connectivity to information and computing power while en route or at a new location. This allows continued productivity and timely response for matters requiring immediate attention. This also reduces the need for assigned offices, potentially decreasing costs associated with desktop technology (e.g., computers, phones), office management, and facility space. DoD, in partnership with industry and the academic community, must continue to advance mobile infrastructure capabilities through the expansion of wireless networks, the evolution of spectrum management, and the establishment of a wireless security architecture.

Objective 1: Evolve spectrum management.

Electromagnetic spectrum is a finite natural resource. The expansion of wireless networks and a growing population of mobile device users place new burdens on spectrum and spectrum management business processes. DoD must rapidly evolve the management of spectrum, which includes businesses processes and associated spectrum data and capabilities, to accommodate new demand within the limitation of DoD's continued reductions in spectrum allocation. Additionally, DoD, in partnership with the academic community, must research methods and technologies to maximize the use of available spectrum (e.g., dynamic spectrum access, smart antennas, innovative multiple access techniques, spectrum sharing technologies) and develop mechanisms for rapidly transitioning technologies into programs of record.

Objective 2: Expand infrastructure to support wireless capabilities.

DoD's evolving enterprise infrastructure and wireless networks need to support unclassified and classified high-bandwidth traffic, mission-critical wireless coverage to in-building and terrestrial environments, and various networking architectures (e.g., heterogeneous networking, carrier aggregation, mobile ad-hoc networks, fixed-mobile convergence, and self-organizing networks). This evolution must leverage industry infrastructure, emerging technologies, and commercial-off-the-shelf products in accordance with policy and standards. For example, DoD must continue to expand its wireless network presence in areas deemed critical for mobile device access through the use of industry-accepted networking standards such as IEEE 802.11-based WLAN networks and 3GPP LTE-based 4G commercial cellular infrastructures. DoD must integrate Telecommunications Expense Management-type solutions to achieve efficiencies with cellular communications. DoD must shape emerging standards by participating in wireless networking standards-related bodies (e.g., TeleManagment Forum, IEEE Dynamic Spectrum Access Networks Standards Committee, and IEEE 802.XX). Additionally, DoD must continue to evolve persistent VPN technologies to ensure that mission critical mobile applications experience continuous connectivity through the use of advanced commercial and DoD network

technologies. For tactical mobile device usage, DoD must mitigate the bandwidth limitations associated with current secured tactical communication methods.

Objective 3: Establish a mobile device security architecture.

Mobile devices expand the boundary of threat. Their growing numbers make them targets for traditional security risks (e.g., viruses, spam, worms, and Trojans) as well as sophisticated new forms of attack. Mobile device use of third-party and commercial wireless networks and short range networks like Bluetooth introduce additional vulnerabilities that must be mitigated. DoD must develop a wireless security architecture that mitigates the risks of mobile device exploitation while leveraging new and emerging technical capabilities. The architecture must enable the management of mobile devices, applications, and network connections to secure the interfaces between DoD networks and commercial networks. Additionally, it must employ DoD Public Key Infrastructure security, access, and identification controls at the network, device, and application levels.

Goal 2: Institute Mobile Device Policies and Standards

The piloting and use of mobile devices continue to grow at a rapid pace as DoD Components seek to provide their workforce with the benefits of mobile technology. Although achieving pockets of success, this unconstrained piloting has also resulted in the lack of security and interoperability across products. Pilots exploring common technologies need to be coordinated to ensure security and interoperability consistency and to achieve greater efficiencies in time and resources. As such, DoD must institute policies and standards to ensure the secure adoption and proper piloting and use of mobile devices. These policies and standards must support the fluid and dynamic nature of mobile technology, enable timely deployment, and provide a means for robust management and compliance validation.

Objective 1: Develop mobile device policy and standards.

Commercial mobile devices make up a majority of the products being piloted and employed across DoD. Commercial mobile devices run operating systems like Apple iOS, Google Android, Google ChromeOS, RIM BlackBerry, RIM QNX, Windows Phone7, and SymbianOS. They target the consumer market with an expectation of leveraging one or more commercial wireless networks. Although the use of commercial mobile devices is more cost-effective than developing customized devices, most do not come equipped out-of-the-box with the security controls, access protocols, and necessary security features required by DoD. This presents undue risk to the enterprise. DoD must develop policy and standards to guide the secure, yet rapid, adoption of commercial mobile devices and to support the consistent and transparent application of security and interoperability requirements. DoD must streamline the approval processes for commercial mobile devices to enable timely deployment and use of this constantly evolving technology. DoD must continue to explore the efficiencies associated with the use of personally-owned mobile devices and potential security risks posed by such devices. Subsequently, DoD must define acceptable uses of personally-owned mobile devices and acceptable personal use of DoD-owned devices where applicable.

Objective 2: Establish a mobile device management service.

As end user dependence on mobile devices rises, enterprise management becomes necessary to ensure continuous and secure mobile device operation and maintenance in a cost-efficient manner. Mobile device management monitors mobile devices deployed across mobile operators, service providers, and enterprises. It provides policy enforcement, integrity validation, device auditing, and as appropriate, peripheral monitoring. Additionally, it includes the following: over-the-air electronic software distribution of data, application, and configuration settings; management of enterprise licenses; and device client registration, asset, and expense management. DoD must establish a federated mobile device management service to optimize operation and maintenance, to enhance security while maintaining compliance, and to support device synchronization. This service must be based on enterprise and user requirements. DoD must plan for mobile device access control, encryption, malware detection, routine backups, regular device scans, security updates, system patches, and the implementation of remote block/wipe tools with minimal impact to mobile device performance. DoD networks must incorporate continuous monitoring technologies to ensure compliance with policies and the protection of DoD information.

Objective 3: Educate and train mobile device users.

The use of mobile devices requires a new level of trust with the end user. DoD personnel, accustomed to using mobile devices in their personal lives, must be aware of the differences when employing the device for DoD mission purposes. Additionally, many critical security controls for mobile devices, especially commercial devices, may only be implementable through User Based Enforcement where the settings are controlled by the user rather than a security policy server. DoD must develop programs that evaluate end user compliance with User Based Enforcement requirements. DoD must educate and train the workforce on the appropriate use of mobile devices and applications for work-related functions and on how to correctly set User Based Enforcement-controlled security settings. To ensure an understanding of why security settings are important, DoD must broadly integrate mobile device training into existing workforce education and training programs where applicable.

Goal 3: Promote the Development and Use of DoD Mobile and Web-Enabled Applications

Similar to software on a desktop computer, mobile applications (or apps) provide enhanced functionality to the end user. Pockets of testing and experimentation demonstrate the potential promise of DoD mobile apps. The chief appeal of DoD mobile apps is low-cost, often faster development and delivery of simple but useful function to the warfighter and/or support personnel. DoD must promote the development and use of mobile apps to quickly deliver function to DoD mobile device users in a secure and interoperable manner. DoD must provide the processes and tools to facilitate app development in

> The House Armed Services Committee Subcommittee on Emerging Threats and Capabilities directed "…the DoD Chief Information Officer to develop and issue a DoD Instruction within 180 days after the day of enactment of [the FY12 National Defense Authorization Act] to clarify the process for developing and using mobile applications on DoD networks."

alignment with policy and standards and to harness the value of individual development efforts for the benefit of the enterprise.

Objective 1: Establish a common mobile application development framework.

A common mobile application development framework consists of developer tools, documentation, and automated processes to help build and test mobile apps. Commercial software development kits provide this capability; however, they are typically operating system-specific. DoD must establish a common mobile application development framework to enable interoperability across operating systems. The framework must leverage commercial capabilities, drive the use of standards, ensure compliance with security requirements, and facilitate consistency among core functions. It may consist of guidance showing DoD Components how to consistently use commercial software development kits, how to apply standard testing criteria, how to port an application to any supported operating system platform, and/or how to sign developed apps with an appropriate signature key. Additionally, the framework must continuously evolve in alignment with industry advancements.

Objective 2: Institute a mobile application certification process.

DoD certification denotes compliance with enterprise networthiness requirements to include security requirements for deployment on DoD networks. It confirms the secure signing of apps, which ensures that malware and viruses were not embedded in the app after signature, and provides acceptable assurance that apps are free from exploitable vulnerabilities. It validates the compatibility and consistent performance of the platform and enforces common formats for data exchange. Additionally, it prohibits the transferring of user and DoD data to non-DoD servers and devices. Current DoD certification processes do not sufficiently support the timely deployment of mobile apps. DoD must institute a streamlined certification process in accordance with policy to support the rapid, automated deployment of mobile apps. DoD must employ remote scanning and continuous monitoring to enforce compliance and to validate application and device integrity.

Objective 3: Provide an enterprise mobile application environment.

An enterprise mobile application environment provides federated and centralized hosting, a certification and approval process, and distribution and management services for mobile apps. A centralized application environment promotes the discoverability and reuse of DoD-approved mobile apps by a greater audience and potentially reduces costs associated with operating and maintaining multiple application hosting environments. Additionally, it eases the tracking of mobile apps for improved lifecycle management (e.g., track enterprise usage to determine if applications require update, maintenance, or discontinued sustainment). DoD must provide an enterprise mobile application environment in alignment with industry best practices to support developers in quickly publishing mobile apps and users in quickly accessing those apps. Considerations for this environment must include the submission process, development process, certification and approval process, management processes, compliance process, and a lifecycle cost model.

Objective 4: "Web-enable" IT capabilities for mobile device support.

A growing mobile workforce requires that current and future IT capabilities (i.e., systems, applications, and services) be architected with mobility in mind to mitigate costs associated with

"retrofitting" capabilities downstream. IT capability developers and service providers must web-enable their products for their inevitable use on mobile devices. This includes special considerations regarding display/presentation capabilities, user interface elements (e.g., touch screen), "mobile-enhanced" technology (e.g., global positioning, gyroscopes/accelerometers), impact on spectrum requirements, and ad hoc and intermittent network connectivity. Additionally, DoD must standardize the security controls, process, and enablement of web-enabled capabilities and applications.

Implementation Considerations Based on Type of User

In deploying mobile devices, DoD must consider the type of user and the nature of the function. The three broad categories of users include enterprise-wide, executive, and tactical support. Enterprise-wide represents the day-to-day functions performed by a majority of DoD personnel to support administrative and general communication (voice, video, or data) activities. Executive represents the information sharing and communication functions required by the highest levels of DoD leaders to make mission critical decisions. Tactical support represents battlefield or mission critical functions needed by warfighters to obtain the operational advantage. These mobile users may require access to information at various classification levels (e.g., non-sensitive, controlled unclassified information, secret, and top secret or above) and in environments ranging in network availability and terrain conditions (e.g., ship, aircraft, or adversarial territories).

Exhibit 2 identifies implementation considerations associated with each user category. Security hardening increases across classifications regardless of user type and enterprise-wide considerations also apply at the executive and tactical support levels.

User Category		Implementation Considerations			
		NON-SENSITIVE	CUI	SECRET	TOP SECRET
Enterprise-wide	Security		Increased Hardening • Encryption • Federal Information Processing Standards		
	Transport	• Network control	• Broadband service • Quality of service		
	Gateways		• Interoperable access • Redundancy • Cross domain support		
	Mission Critical Services		• Low latency • High availability • Robust cellular roaming / persistent connectivity		
	Mobile Device Management	• Auditing • CMD peripheral control (Camera/ GPS/ Wi-Fi/etc.)	• Auditing • Data-at-rest / data-in-transit encryption • Remote wipe • Strong authentication • CMD peripheral control (Camera/GPS/Wi-Fi/etc.)		
	Application Management	• Approved commercial apps • Application control	• Validated apps • Application authorization • Centralized app store		
Executive		• Network control	• Priority access • Gateway(s) to C2 networks		
Tactical Support		• Network control	• Ruggedized device • Delay tolerant networking • Selective availability anti-spoofing • Transmission security • Anti-jam • Spectrum • Interoperability • Phase of conflict • Removal of fixed infrastructure vulnerability		

Exhibit 2: Implementation Considerations

In addition to the considerations in Exhibit 2, DoD must consider complementary initiatives such as identity and access management and cloud computing efforts as well as the impact to force protection in the deployment of mobile devices. Pilots and policy activities must continue to explore and refine implementation strategies based on capability-type requirements.

Next Steps

The DoD Mobile Device Strategy identifies the IT goals and objectives for maximizing the use of mobile devices and apps in the DoD Information Enterprise. An implementation plan will follow, which will initially support small user populations to assess the efficacy of the strategy. By validating productivity gains, reviewing security architectures, and managing a small segment of users, a business case can be developed that may support scaling to an enterprise-wide solution. Additionally, DoD will develop a communication strategy to include outreach via conventional and contemporary methods for addressing the acquisition and cultural challenges associated with enterprise-wide mobile device adoption and deployment. DoD Components shall participate in the DoD CIO Commercial Mobile Device Working Group (CMDWG) to share pilot activities, best practices, lessons learned, and efficiencies.

As the DoD Information Enterprise matures to accommodate mobile devices, DoD will continue to explore emerging technologies maintaining the notion that tomorrow's information enterprise may look very different from today's.