DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

SAIS-CB

NOV 21 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Mobility Strategy

1. References:

a. Memorandum, Department of Defense (DoD) Chief Information Officer (CIO), 8 June 2012, subject: Department of Defense Mobile Strategy.

b. Memorandum, DoD CIO, 15 February 2013, subject: Department of Defense Commercial Mobile Device Implementation Plan.

c. Memorandum, DoD CIO, 21 March 2013, subject: Department of Defense Commercial Mobile Device Pilot Consolidation.

d. Army Regulation (AR) 25-1, Army Information Technology, 25 June 2013.

e. Army Regulation (AR) 25-2, Information Assurance, Rapid Action Revision, 23 March 2009.

f. Memorandum, Under Secretary of the Army, 10 May 2013, subject: Commander and Leader Responsibilities for Cyber Security/Information Assurance (CS/IA) Incidents.

g. Memorandum, Secretary of the Army, 11 March 2013, subject: Army Directive 2013-02 (Network 2020 and Beyond: The Way Ahead).

h. Information Technology Management Reform Implementation Plan, signed by the Secretary of the Army 20 February 2013.

i. Digital Government Strategy 2012.

j. Executive Order 13589, Promoting Efficient Spending, November 2011.

2. **Purpose.** This memorandum communicates the Army's strategic vision for utilizing mobile capabilities. The Army's first priority for mobility is to enable mission accomplishment. From strategic policy development to tactical operations, the potential for smart mobile devices to strengthen the Army workforce is tremendous. The mobile workforce's ability to access information and computing power, anywhere at any time, will

improve information sharing, communication and action response time, leading to greater mission effectiveness. The Army's second priority for mobility is to produce efficiencies and innovations. In a fiscally constrained environment, the Army needs to add smart mobile capabilities while reducing the total cost of ownership (TCO) as part of an overall cost-reduction strategy. With these goals in mind, over time the enterprise information environment will evolve to capitalize on the use of smart mobile devices.

3. **Alignment to DoD and Federal Strategy.** The overarching document guiding the Army Mobility Strategy is the DoD Mobile Device Strategy (2012). The DoD strategy focuses on improving three areas critical to mobility: wireless infrastructure, the smart mobile device itself, and smart mobile applications. It allows mobile activities across DoD to converge toward a common vision, and mandates a single enterprise approach for smart mobile IT. The Army Mobility Strategy will closely align with the DoD strategy as it evolves. The Army Mobility Strategy also will adhere to the efficient spending principles of the Information Technology Management Reform Implementation Plan as well as government-wide initiatives, such as the Digital Government Strategy and Executive Order 13589 (Promoting Efficient Spending). To ensure that the strategy remains current and satisfies DoD and Federal policies, the Army will maintain situational awareness of legislative efforts and best practices in private industry, other government agencies and its sister Services.

4. **Enterprise Infrastructure for Mobile Devices.** A wireless infrastructure frees the user from the confines of a desk. Equipped with a mobile device, the user will be able to maintain connectivity to information and computing power while en route or at a new location, improving productivity and timely response to matters requiring immediate attention. Mobile devices also reduce 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.

a. *Evolve spectrum management*. DISA and the program management office will be responsible for spectrum management development. Electromagnetic spectrum is a finite natural resource. The expansion of wireless networks and a growing population of smart mobile device users place new burdens on spectrum and spectrum management business processes. DoD must rapidly evolve the management of spectrum, including business processes and associated spectrum data and capabilities, to accommodate new demand for spectrum allocation. With the academic community, DoD also 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. In the tactical environment, DoD must ensure the availability of secure spectrum in a contested space vulnerable to Blue and/or Red Force jamming or spoofing.

b. *Expand wireless infrastructure*. DoD's evolving enterprise infrastructure and wireless networks need to support unclassified and classified high-bandwidth traffic. In conjunction, the Army must extend mission-critical wireless coverage to in-building and terrestrial environments, various networking architectures, and low-bandwidth disadvantaged deployed tactical network 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, the Army is assessing smart mobile technology similar to that on 3G- and 4G-based commercial cellular infrastructures. DoD must integrate telecommunications expense management-type solutions to achieve efficiencies with cellular communications. DoD also must shape emerging standards by participating in wireless networking standards-related bodies. Additionally, DoD must continue to evolve persistent VPN technologies to ensure that mission-critical smart mobile applications have continuous connectivity. In the tactical environment, smart mobile devices have the potential to mitigate the bandwidth limitations associated with current secure tactical communication methods. To effectively utilize smart mobile devices in the tactical environment, DoD will need to address the availability and security of wireless infrastructure (understanding when to deploy appropriate DoD infrastructure) and the security and functionality of the smart mobile devices.

c. *Establish mobile security architecture*. Smart mobile devices expand the threat boundary. Mobile devices can be targets of traditional security risks, such as viruses, spam, worms and Trojans, as well as sophisticated new forms of attack. Smart mobile device use via third-party and commercial wireless networks and short-range networks, such as Bluetooth, introduces additional vulnerabilities and risks that need to be corrected or mitigated. DoD must develop a wireless security architecture that mitigates the risks of smart mobile device exploitation while leveraging new and emerging technical capabilities. The architecture must enable the management of smart mobile devices, applications and network connections to secure interfaces between DoD and commercial networks, employing access-identification controls to protect and secure data at rest (DAR), and DoD Public Key Infrastructure security, access and identification controls at the network, device and application levels. The architecture also must address the unique demands of the tactical operating environment and the need to maintain security and control in low-bandwidth and bandwidth-denied operating conditions.

5. **Mobile Device Policies and Standards.** The piloting and use of smart mobile devices continue to grow at a rapid pace as Army organizations seek to provide the workforce the benefits of smart mobile technology. These technology assessments provide benefits in terms of enhanced capabilities, but also include security and interoperability challenges. Moving forward to fully explore and leverage these emerging technologies will require coordination to ensure security implementation, integration and consistent interoperability to achieve efficiencies and reduce cost in time and resources. The Army must institute policies and standards to ensure the secure adoption and proper piloting and use of smart mobile devices. These policies and standards must support the fluid and dynamic nature of

smart mobile technology, enable timely deployment and provide a means for robust management and compliance validation.

a. *Develop mobile policy documents.* Army and DISA will be modifying and updating existing acceptable personal use policies for GFE smart mobile devices. DISA procurement of Mobile Device Management (MDM) and the Mobile Application Store will provide the baseline for approving the hardware and software development of devices that will connect to the Global Information Grid (GIG). The policy will address acceptable use of commercial smart mobile devices when and where applicable. These devices are not equipped out-of-the-box with the security functions and necessary features required by DoD. This presents risk to the enterprise. Army 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 smart mobile devices to enable timely deployment and use of this constantly evolving technology.

b. *Establish mobile device management.* As end-user dependence on smart mobile devices rises, enterprise management becomes necessary to ensure continuous and secure smart mobile device operation and maintenance in a cost-efficient manner. Smart 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: 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 is establishing a mobile device management service to optimize operation and maintenance, to enhance security while maintaining compliance, and to support device synchronization. As part of the DoD CIO-mandated single enterprise solution, organizations must plan for smart mobile device access control, encryption, malware detection, routine backup, regular device scans, security updates, system patches and implementation of remote block/wipe tools with minimal impact to performance. Networks must incorporate continuous monitoring technologies for mobile devices to ensure policy compliance and the protection of information. Mobile Device Management must accommodate the more critical nature and unique requirements of executive and classified smart mobile devices in the strategic environment. This will require the ability to maintain security and control in low-bandwidth and bandwidth-denied operating conditions.

c. *Educate mobile users.* The use of smart mobile devices requires a new level of trust with the end user. Army personnel, accustomed to using smart mobile devices in their personal lives, must be aware of the differences when employing the device for Army mission purposes. Additionally, many critical security controls for smart mobile devices, especially commercial devices, may only be implemented through user-based enforcement where the user, rather than a security policy server, controls the settings. The Army must develop programs that evaluate end-user compliance with user-based enforcement requirements. The Army also must educate and train the workforce regarding the appropriate use of smart mobile devices and applications for work-related functions and

how to correctly set user-based enforcement security settings. To ensure an understanding of why security settings are important, the Army must broadly integrate smart mobile device training into existing workforce education and training programs.

6. **Mobile Applications.** Similar to software on a desktop computer, smart mobile applications (or apps) provide enhanced functionality to the end user. The chief appeal of Army smart mobile apps is low-cost, often faster development and delivery of simple but useful functions to the warfighter and/or support personnel. As data and information are made available to commercial mobile devices (CMD), it will become necessary to have applications in place that will present that data and offer the capabilities necessary to read, change, save and access the data. Managing these applications involves governance, compliance, sustainment and proper use of the application and the data the application has the permission to access. The processes for vetting, approving, authorizing, deploying and sustaining applications are being developed for both the Army and DoD. The Mobile Application Store (MAS) will execute deployment.

a. *Establish mobile application development framework.* A common smart mobile application development framework consists of developer tools, documentation and automated processes to help build and test smart mobile apps. Commercial software-development kits provide this capability; however, they are typically operating system specific. DoD must establish a common smart 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. The smart mobile application development framework must augment commercial capabilities with methods to meet federal and DoD-specific requirements, such as those required by the Privacy Act for the safeguarding of Personally Identifiable Information, compliance with the Section 508 Amendment to the Rehabilitation Act of 1973, etc. These methods may consist of guidance showing DoD Components how to demonstrate the use of commercial software development kits, apply standard testing criteria and port an application to any supported operating system. The framework must continuously evolve with industry advancements.

b. *Establish 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 do not become embedded in the app after signature. This 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 transfer of user and DoD data to non-DoD servers and devices. DoD must leverage a streamlined certification process, to support the rapid, automated deployment of smart mobile apps. Acceptance of certified smart mobile apps through a DoD-wide reciprocity program is crucial to building a DoD certification process that can support the timely deployment of smart mobile apps required by the Army and the other services.

c. *Establish mobile application management system.* The Mobile Application Store provides federated and centralized hosting, a certification and approval process, distribution and management services, and sustainment and retirement services for smart mobile apps. A centralized application environment promotes the discoverability and reuse of DoD-approved smart 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 smart mobile apps for improved life-cycle management. All applications will be vetted, approved and authorized prior to being made available to the user. The Mobile Application Store must also provide the ability to change, restrict or revoke applications as required.

d. *Web-enabled IT capabilities for use by mobile devices.* A growing smart 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 the inevitable use on smart mobile devices. This includes special considerations regarding display/presentation capabilities, user interface elements (e.g., touch screen), 508 compliance, mobile-enhanced technology, impact on spectrum, and ad hoc and intermittent network connectivity as part of standardized security controls, processes and use of web-enabled capabilities.

7. **Mobile Device Life-Cycle Management.** The plan for managing CMDs must be a holistic, cradle-to-grave approach. It must include rapid mobile device acquisition, configuration and deployment, maintenance and support, and sanitization and disposal. Tradeoffs must be addressed within each area before a management strategy can be established.

8. **Classified Mobile Devices.** The Army secure mobility effort focuses on the evolution and development of a scalable, secure, smart, mobile communications capability founded on commercial technologies aligned with National Security Agency guidance. The NSA is developing scalable mobility capability packages and protection profiles in line with the NSA Commercial Solutions for Classified (CSfC) strategy. CSfC enables commercial products to be used in layered solutions to protect classified National Security Systems (NSS) data. This approach will enable the Army to provide secure communications based on commercial standards that can be fielded in months, not years. The Army strategy for protecting classified information employs both commercial off-the-shelf and government off-the-shelf information assurance solutions to meet customer needs. The Army is collaborating with DISA, the NSA, the DoD CIO and the Joint Staff to configure and test prototype secure 4G mobile solutions. Near-term efforts include WIN-T Increment 2 experimentation with tactical 4G integration. TRADOC is working this effort in direct response to a network modernization directed requirement as a bridge to a draft Capability Production Document. The Army Rapid Equipping Force and Nett Warrior are also working with the Joint Capability Technology Demonstration Joint Operational Long-Term Evolution Deployable – Tactical Cellular System (JOLTED TACTICS) to test a prototype secure 4G tactical mobile data and voice solution. Lessons learned from current efforts may warrant

additional requirements analysis to address the integration of information assurance and security efforts. The Army will continue to engage several technology assessment methodologies, which are reflected throughout this document.

9. **Tactical Mobile Devices**. The Army continues working alongside several of the Secure Mobility Strategic for Classified (SMfC) and Tactical Mobility for Classified (TMfC) pilots and operational assessments. This includes programs of record, such as the Joint Tactical Radio System, WIN-T Increment 2, Nett Warrior, Joint Battle Command - Platform and Blue Force Tracking. The Army is also participating in JOLTED TACTICS, which provides a tactically deployable cellular (broadband) capability to support secure information sharing (voice, video, data and applications) among aerial, fixed ground, mobile and maritime platforms. Nett Warrior (formerly known as Ground Soldier System) is an integrated dismounted leader situational awareness system for combat operations. Nett Warrior was fielded to the 101st Airborne, 82nd Airborne, and 10th Mountain divisions to support Combat Support Capability Set 13/14. To overcome integration challenges between strategic mobility and tactical mobility, 4G/LTE capability requirements for the tactical environment will require further analysis. The goal is to develop a Capability Production Document (CPD) based on product-neutral information. The CPD will be submitted to the NSA via JOLTED TACTICS to be validated against the CSfC. Integrators will develop a secure, compliant solution by selecting commercial products based on the CPD and CSfC guidance.

10. **Way Ahead for Army Mobility**. The DoD CIO and DISA are continuing to develop plans for implementing all aspects of mobility. The Army is constantly synchronizing with this development and remains a key contributor. In order to define our direction in an ever-changing mobility climate, the following areas will continue to be addressed with both the DISA program management office and the Army mobility leads: risk tolerance for mobile devices, mobile device life-cycle management, and the feasibility of a "bring your own device" program for mobile devices. Finally, the Army will publish an implementation plan in FY14 to provide actionable details to subordinate commands and agencies.

11. The point of contact for this action is Mr. Rick Walsh: (703) 545-1598 or john.r.walsh46.civ@mail.mil.

MICHAEL E. KRIEGER
Acting Chief Information Officer/G-6

SAIS-CB
SUBJECT: Army Mobility Strategy

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade

CF:
Army Information Assurance Program Managers
Director, Army National Guard
Director of Business Transformation