RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL STEVEN W. BOUTELLE, USA
CHIEF INFORMATION OFFICER/G-6,
UNITED STATES ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
UNITED STATES HOUSE OF REPRESENTATIVES

SECOND SESSION, 109TH CONGRESS

INFORMATION TECHNOLOGY

APRIL 6, 2006

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Lieutenant General Steven W. Boutelle, USA
Chief Information Officer/G-6,
United States Army

Good afternoon, Mr. Chairman and distinguished members of the subcommittee. I am Lieutenant General Steven Boutelle, the Chief Information Officer (CIO) and G-6 for the U.S. Army. I am pleased to appear before the subcommittee today to discuss the Army's Information Technology (IT) efforts and how we are using IT to enable our Soldiers to fight the Global War on Terrorism (GWOT).

As you know, IT is more than just the computer on your desk that you create documents with, send and receive e-mail on, and surf the web with. It's the cable that connects your computer to the larger network within this building and eventually to the Global Information Grid (GIG). It's the commercial and military satellites that allow forward deployed Soldiers, Sailors, Airmen and Marines to reach back to their home stations for critical logistical and intelligence support. It's the applications and protocols that move the data from one point to another. Information Technology is the key to providing persistent connectivity - connecting Soldiers with critical information, weapons systems, sensors and the sustaining base.

The Secretary of the Army, during his welcoming remarks on December 6, 2004, clearly articulated how important information technology is for the Army: "The technology that is at the center of Transformation is Information Technology. The long term goal of the Information Age Transformation of the Department of Defense is an

organization that is capable of conducting Network Centric Operations, both military and business, in a totally joint fashion, to include our allies and partners. From the military point of view, a network centric capable force is one that is robustly networked (including command and control, warfighters, platforms, and sensors), fully interoperable and shares information and collaborates by means of a communications and information infrastructure that is global, secure, real time, reliable, internet-based, and user-driven."

The recent Quadrennial Defense Review's top-down review emphasized the criticality of five main areas - information assurance (IA), information sharing, data strategy, common enterprise services, and infrastructure/transport (aka military satellite communications). Each is of vital importance to the Army and the Department of Defense (DoD). This is reflected in our ongoing strategy to upgrade our networks with hardware and software; to move away from our legacy systems to a more mobile and deployable, and interoperable environment.

Today's Army is deployed to over 120 countries. In Iraq and elsewhere, IT is a big part of how today's combat Soldiers now fight in traditional battles and in battles waged on our networks. Our Soldiers must be ready to maneuver network assets throughout the battlespace in real time, and they must be able to wield this IT to support a joint force commander. To succeed, commanders and Soldiers must have a full suite of network capabilities - in garrison, en route to destination, and when deployed. War today is as part of a joint force and, frequently, as part of a coalition. Interoperability exists today at the network level and extends through space-based and terrestrial transmission systems. All new

systems must have joint interoperability and enable network interdependencies.

The Army is working arm-in-arm with its sister services to develop the network elements of the Defense Department's GIG. We have migrated to commercial standards and Web technologies to further strengthen interoperability. The Army has nearly completed the migration to an Internet Protocol or IP-based network as part of the larger joint defense network, and we're moving to IP Version 6 for a more efficient and interoperable network.

Today, all of DoD is moving to converged IP, merging voice, data and video services. The result is faster, more efficient bandwidth use, a smaller footprint and a reduction in the number of people needed to operate the equipment. The Joint Communications Support Element at MacDill Air Force Base, Florida, led the way with its everything-over-IP approach. They have proven that it is possible. More than that, convergence is a combat multiplier: It eliminates much of the rigidity of our legacy systems. It's scalable, flexible and cost-efficient. You get more bandwidth out of the same system

But replacing a circuit-based world is complex. To get there, the Army is going from its thirty year old cold war Mobile Subscriber Equipment (MSE) to the IP-based Joint Network Node (JNN). We're simultaneously preparing to field the DoD Warfighter Information Network-Tactical (WIN-T), Joint Tactical Radio System (JTRS), Transformational Communications System, GIG-Bandwidth Expansion and Net-Centric Enterprise Services (NCES). The Army is rapidly providing mature and

available capabilities of the WIN-T program to Soldiers through the Joint Network Transport Capability-Spiral initiative. These programs-along with the Army's Installation Information Infrastructure Modernization Program (I3MP), will make it possible to support deployed forces from foxhole to home station.

The JNN provides a significant increase in capability to Army modular units by providing satellite based high bandwidth (4 megabits per second (Mbps)) down to the battalion level whereas the previous MSE system only provided limited bandwidth and stopped at the brigade level. The JNN provides the brigade combat team (BCT) headquarters not only the 4 Mbps on its IP mesh network but another 3 Mbps on its joint circuit network. This provides commanders with unprecedented capability for real-time command and control at the quick halt while operating over a geographically dispersed area. The Army has fielded JNNs to 7 of 10 active Army divisions and plans include near term fielding to the remaining three active Army divisions as well as brigade sized deploying units to include Army Reserve and the Army National Guard units. The JNN was demonstrated and achieved great successes in the nation's largest national disaster, Katrina.

The Army is also constructing Regional Hub Nodes, collocated in DoD's Teleports, in support of the satellite-based command and control systems being fielded to Army divisions and BCTs. The first regional hub will be constructed starting in FY06 in the Central Command theater to support Army units in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF). Additional hubs will be started in FY 07 for U.S. Army Europe and US Army Pacific. These hubs give significant

expeditionary capability by allowing individual BCTs to deploy and install their tactical networks at a moments notice without the need for the pre-positioning of the division tactical JNN hub node. The regional hub nodes provide network connectivity flexibility and scalability to commanders.

With the JNN, the Army is solving the near-term GWOT communications problems experienced during the initial stages of OIF by taking advantage of technology convergence using IP technology.

WIN-T is the tactical communications backbone for today's and tomorrow's warfighter because it provides increased capacity and operational flexibility over the JNN. WIN-T must not only support a wide variety of warfighter-driven applications, but will also support and enhance those programs that provide access-capabilities, such as Future Combat Systems (FCS) and JTRS. WIN-T accomplishes these objectives through precision blending of multiple commercial-off-the-shelf technologies and capabilities.

JTRS is the next generation family of tactical radios that moves the Army from single purpose radios to multi-band, multi-mode software programmable digital radios to transport the warfighter's command and control requirements. JTRS is planned as an integral part of Army Future Force operations and in concert with WIN-T, will ensure seamless information operations within the Global GIG. JTRS Ground Mobile Radio (GMR), formerly Cluster 1, and Handheld, Manpack and Small Form Fit (HMS) radios, formerly Cluster 5, consists of a networking capability that is essential to the Army's FCS communications network provided through Soldier Radio Waveform and Wideband Network Waveform. While the

GMR supports the Army's ground vehicular requirement, the HMS radio satisfies the handheld, manpack, and small form-fit requirements supporting FCS and Land Warrior.

I3MP is the Army's premier communications modernization program that provides the last mile of connectivity for the sustaining base. The I3MP installs fiber optic and wireless information transport systems along with the hardware and software required to ensure the installation has the most efficient, interoperable, commercially standard technology available. Beginning this fiscal year, the program will focus directly on those installations housing and supporting modular units, including their training and support activities. These improvements will support combat force readiness by meeting the information requirements of deploying, deployed, and returning warfighting forces.

I3MP funds provide for the establishment of several Area Processing Centers (APC). These centers will host services for the entire array of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medical, and military personnel readiness. In addition to providing enhanced reachback capability to deployed forces, the consolidation of IT investments and operating resources typically located on every Army installation will reduce operating costs and enhance the Army's ability to secure its networks. This will be accomplished by moving vulnerabilities typically located at every installation to APCs that are equipped with expanded IA and computer network defense capabilities. The robust secure architecture that is typically built into over 190 installations will now be consolidated into under ten APCs, reducing the number of entry points into Army

networks. The APCs should be consolidated in Defense Information Systems Agency's (DISA) data mega centers.

The Army CIO/G-6 is the Executive Agent for DoD Biometrics, responsible for leading, coordinating, and consolidating the integration of biometric technologies across the DoD. To support the overall efforts in the GWOT and homeland defense, DoD Biometrics works within the DoD and with other U.S. government organizations, including the White House National Science and Technology Council's Subcommittee on Biometrics, the U.S. Technical Advisory Group on Biometric Standards, and the Biometric Consortium.

It is increasingly important for the DoD to leverage biometric technologies so that military units can link an individual encountered in a hostile or potentially dangerous environment to that individual's previously used names, aliases, and prior activities. For example, biometrics has enabled the identification of bomb makers in the counter-improvised explosive devices targeting program. This direct support to our Warfighters has been effective because of the development of a biometric matching capability modeled on the FBI system, and information-sharing efforts with external DoD and U.S. government organizations. There are several biometric collection systems that together are responsible for the tens of thousands of matches made to date - 42,376 as of March 31, 2006.

Biometrics is a growth industry in supporting the GWOT. Biometrics has made significant progress to date to include establishing a

biometric enterprise matching capability that is interoperable with the FBI based on existing standards. Also, Biometrics has led the U.S. government in biometric standards development. Biometrics has increased the force protection capabilities for U.S. forces in Iraq. Biometrics is about reliable identification.

The Army relies heavily on its networks for information superiority and the conduct of combat operations. Therefore, it is critical that the network and the data on it be protected. The Army has several successful approaches for reducing vulnerabilities to its networks and protecting against internal and external cyber-terrorists (nation states, non state actors, criminal enterprises) and malicious threats, and unintentional user errors. These include integration of a robust public key architecture, digital signature capabilities, and technical solutions to ensure identity and system authentication and verification.

IA is the foundational pillar of information dominance in a net-centric warfare environment. It assures that the Army's LandWarNet can provide reliable communications for a global force. Several key IA priorities significantly enhance the security of Army networks, systems, assuring software pedigree and suppliers, protecting data and privacy, and advance information sharing across communication domains with partners from service agencies, allies, and coalition:

- The IA Policy and Compliance Program is a proactive risk management-based defense-in-depth strategy to defend against external and internal threats to Army information systems, networks, and data. The program develops, promulgates, and enforces IA policies, processes, best

practices, and compliance to include: Federal Information Security Management Act, Army certification and accreditation, net worthiness, and cryptographic and key management modernization programs.

- IA tools policy and processes streamline and provide baseline requirements to the commercial industry, acquisition, integrators and testing communities. Vetting tools, products, and manufacturers through a structured process allows Army suppliers, vendors, acquisition decision makers, and integrators to harmonize IA requirements for design, development, selection, and deployment of best of breed technology that is risk and threat free and conforms to federal, national, and defense standards.

A major vulnerability to the network has always been the use of passwords. The use of a token-based approach for network access significantly reduces the risk of network access by unauthorized personnel. The Army continues to be an active leader as DoD migrates to the interoperable, Personal Identification Verification card. The current DoD Common Access Card (CAC) is the approved Homeland Security Presidential Directive (HSPD) -12 compliant credential. The effort began in October 2005 with the Common Access Card Cryptographic Logon (CCL) and will continue in phased implementation plans toward achieving compliance with HSPD-12 mandates. The Army successfully began implementing its CCL for two factor authentication in December 2005 and will conclude in June 2006.

The Army is now working on the last impediment to achieving true interoperability – data strategy to improve information sharing. The network has become a commodity that can be bought off the shelf as you would a computer. We have mastered the transport business, now we have to master the exchange of data.

The Army CIO/G-6 is responsible for developing the strategy, policy, guidance, and roadmap required to promulgate the DoD Net-Centric Data Strategy in the Army. To this end, the CIO/G6 established Net-Centric Data Strategy related policy and is promulgating an enterprise level implementation roadmap. CIO/G-6 is providing data engineering support to several key joint communities of interest (COIs) such as: Blue Force Tracking, Time Sensitive Targeting, joint Net Operations, and DoD Information Management Data. CIO/G6 also supports several Army forums that are addressing information sharing issues e.g., Software Blocking, and Warfighter Mission Area Implementation Working Group. CIO/G-6 in conjunction with the Army Materiel Command is establishing a Net-Centric Data Center of Excellence (CoE) at Fort Monmouth; initial operational capability is targeted for May 2006 with full operational capability expected November 2006. The CoE will provide data management assistance to mission area and domain lead COIs.

The CIO/G-6's net-centric data initiatives have focused on the Warfighter Mission Area because lack of interoperability continues to inhibit modular and expeditionary operations. Data standardization is the key to ensuring interoperability among Army's Battle Command IT systems. A key effort in implementing a DoD Net-Centric Data Strategy is the adoption of the Joint Consultation, Command and Control Information

Exchange Data Model (JC3IEDM). CIO/G-6 leads configuration management of the JC3IEDM. This international standard has been adopted by 26 Nations for coalition interoperability, mandated by DoD as the C2 coalition information exchange standard, adopted by the Marine Corps, the Army's Future Combat System, the DoD Global Force Management system, and others. It is currently under consideration by the Joint Command and Control (JC2) Program. CIO/G-6 provides engineering expertise and advice in the use and implementation of the JC3IEDM in FCS.

The Army is the first DoD Service to endorse an information exchange standard for command and control (C2) and all Army C2 systems will implement the J3CIEDM. CIO/G-6 and the Army G3 are working with Joint Forces Command and the Office of the Joint Chiefs of Staff to ensure JC3IEDM will be used by all DoD Components for C2 information sharing.

The CIO/G-6 has crafted and institutionalized a set of transformational initiatives that help the Army effectively and efficiently fulfill its mission of providing necessary forces and capabilities to the Combatant Commanders in support of the National Security and Defense Strategies.

The first initiative was the establishment of a new governance structure within the Army to effectively manage and deliver required IT-based capabilities. This governance structure has four mission areas and assigned responsibility for them within the Army Staff: (1) Warfighting Mission Area, (2) Business Mission Area, (3) Defense Intelligence Mission

Area, and (4) Enterprise Information Environment Mission Area. The mission areas are further broken down into domains and sub-domains. Governance is accomplished at each level to ensure new IT-based capabilities are synchronized within the Army enterprise. It is being leveraged to reduce duplicative and stove-piped IT-based capabilities by 80% by the end of FY 07 and to reduce the cost of Army operations.

Portfolio management processes were developed for implementation within this new governance structure to assist in the optimal application of funds for acquiring IT-based capabilities. These processes involve conducting periodic portfolio reviews of the mission areas to ensure IT capabilities and investments are synchronized across the Army. Army's IT investments are managed in the newly procured Army Portfolio Management Solution to assist Army mission and domain leads in managing their portfolios.

The governance structure and portfolio management processes were used to develop and author the Army's Business Transformation Plan as part of the DoD's business transformation efforts (formerly the Enterprise Transition Plan), that was delivered to Congress on March 15, 2006. Lean Six Sigma and other industry best practices are being leveraged to increase the Army's agility and adaptability necessary to decrease cycle time in all processes and activities.

Another major initiative is the implementation of commercial-off-the-shelf Enterprise Resource Planning (ERP) applications which can be used to streamline processes previously managed by a plethora of stove-piped systems which severely limit the Army's ability to rapidly adapt its

processes in an environment of continuous change. One such ERP program, General Fund Enterprise Business System , is being implemented with the specific intent of providing the type of financial transparency and cost visibility across the Army enterprise required by commercial and Government organizations wishing to remain agile and comply with either Sarbanes-Oxley or the Chief Financial Officers and Federal Financial Management Improvement Acts.

Lastly, no transformation initiative or process would endure if the workforce is not developed and sensitized to see new programs, systems and initiatives through to completion. For example, the e-Learning Program consists of nearly 2,000 internet-based courses on various specialties in IT, knowledge management, business, governance, and foreign languages. This program is centrally-funded and available to all Army personnel at no extra cost.

Army Knowledge Online (AKO) is the Army's Enterprise Portal and provides access to secure, validated Army knowledge, systems and services from anywhere, at anytime, and from any Web based browser. AKO meets the critical warfighting requirement to quickly and securely share information across the Army. It gets at the heart of several challenges the Services and DoD have been working at for more than a few years – standardization, interoperability, and the breaking down of information stovepipes. AKO enterprise-level services including user authentication, global email, web-based collaboration, file storage, and instant messaging. During a typical month, the highest AKO usage is by units that are deployed to support OIF and OEF.

For AKO to be fully utilized overseas and in the tactical environment, it must be quick and reliable. AKO Forward is an initiative to deploy AKO services at strategic locations around the world to ensure the immediate delivery information to soldiers and supporting organizations. AKO Forward will serve as the Army platform to host standard Army capabilities worldwide - reducing latency and providing improved services to support deployed and OCONUS units. The first site will be in Southwest Asia with an initial operational capability in summer 2006.

AKO is the largest and most mature of all of the DoD portals. Senior Army and DISA leaders saw an opportunity for synergy and directed the development of the Defense Knowledge Online (DKO) portal with associated enterprise-class services. The Air Force, Navy and Marines have all shown interest in the potential for making this a joint effort. The DKO portal will provide the prototype platform for future Core Enterprise Services for DoD. The convergence of AKO and other Service portals to DKO could provide a DoD-wide portal for NCES core services and become the single, daily information source for warfighters and supporting organizations across the DoD Enterprise.

Finally, I would like to highlight that our support to the GWOT is not limited to IT-based solutions and strategies. We are actively involved in aiding the Joint community in developing solutions to combat Improvised Explosives Devices (IEDs) - the current terrorist weapon of choice. For the foreseeable future IEDs will likely remain as a major component of the GWOT. To effectively counter this complex threat, the Joint Improvised Explosives Devices Defeat Organization developed a capability for full spectrum analysis of IEDs that considers and applies multiple materiel,

doctrinal, and training strategies. Unfortunately, the use of some counter IED solutions adversely affects our warfighter's use of communications equipment. The Army is implementing various mitigation techniques with the Joint warfighting community that include: modifying current tactics, techniques and procedures; developing spectrum management tools that more effectively de-conflict the electromagnetic environment; and establishing a forum validate, synchronize and integrate IED and Electronic Warfare solutions. The Army remains committed to ensuring its forces engaged in the GWOT are afforded the best possible force protection systems and measures.

In conclusion, the Army has made significant progress in providing NCES down to the Soldier. We have provided significant increases in bandwidth to the warfighter and at the same time extended the network down to levels never seen before. We continue our support of the WIN-T program while bringing in WIN-T developed technology into the current force. We are migrating to commercial standards with the most significant being the moving to an everything-over-IP environment which has provided increased bandwidth while reducing support requirements. The I3MP is providing critical IT infrastructure to installations to allow them to support forward deployed Soldiers. We are leveraging Biometrics in the GWOT to assist in identifying and apprehending terrorists world wide. We have made significant steps in locking down our networks to protect our critical transformation key enabler – the network. We are working towards improved information sharing intra-Army, with other services and our coalition partners through the development and application of a data strategy. Finally, we have introduced improved business processes to get the most out of our budget dollars, and to ensure they are spent wisely.

But, we are not done. We still have much to do. The Army's IT Budget request for fiscal year 2007 supports the specific initiatives I have discussed today as well many others, all critical in supporting the GWOT. We can provide you with further details.