STATEMENT BY

JOHN G. GRIMES
ASSISTANT SECRETARY OF DEFENSE
(NETWORKS AND INFORMATION INTEGRATION)
AND
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL
THREATS AND CAPABILITIES
HOUSE ARMED SERVICES COMMITTEE

ON

INFORMATION TECHNOLOGY ISSUES AND DEFENSE TRANSFORMATION

APRIL 6, 2006

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM,
UNCONVENTIONAL THREATS AND
CAPABILITIES,
HOUSE ARMED SERVICES COMMITTEE

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on Terrorism, Unconventional Threats and Capabilities on the importance of information technology (IT) to the transformation of the Department of Defense (DoD). I am John Grimes and this is my first opportunity to appear before you as the Assistant Secretary of Defense for Networks and Information Integration and the Department's Chief Information Officer (CIO). My prepared remarks will focus on how the Department is leveraging ever-increasingly capable information technology to deliver the actionable information that we need to deal with new threats to security and stability around the world.

IT is critical to supporting the warfighter and fighting terrorism. Today's warfighter depends on a staggering number of IT systems and information services that feature video, graphics, imagery, collaborative planning tools, remote interactive battlefield operating systems, and systems that rely heavily on geographically distributed databases for their functionality. Evidence of these information transfer requirements are manifested in the bandwidth requirements captured to support the U.S. Central Command (USCENTCOM) area of responsibility (AOR) from Operation Desert Shield to Operation Iraqi Freedom (OIF). From Operation Desert Shield/Desert Storm to September 11, 2001, the bandwidth supporting the USCENTCOM AOR remained relatively constant at 45 megabytes per second (Mbps). By March 2003, supporting a force one-quarter the size of that involved with Operation Desert Shield/Desert Storm, the theater bandwidth requirements increased nearly 5,000 percent and were still growing. Since then, that requirement has grown another 166 percent to approximately 5.9 gigabits per second (GBps). At the same time, the IT budget has remained relatively constant in comparison to the overall Defense budget. The President's fiscal year (FY) 2007 Defense budget request of $439.3 billion represents a seven percent (7%) increase from what was enacted last year, while the Department's FY 2007 IT budget request of $30.9 billion represents a three percent (3%) increase from what was enacted last year ($29.9 billion).

The IT budget reflects Defense Transformation as a key element of the Secretary of Defense's Strategy to meet the challenges of the dangerous and uncertain security environment of the 21st century. In his strategy, the Secretary has identified six critical operational goals that provide the focus for the Department's transformation efforts and in turn the focus of the FY 2007 IT budget:

- Protect critical bases and defeat chemical, biological, radiological, and nuclear weapons.
- Protect and sustain forces in anti-access environment.
- Deny enemies sanctuary.
- Leverage information technology.
- Assure information systems and conducting information operations.
- Enhance space capabilities.

The DoD and the Services have reaped IT benefits similar to the civil sector. Soldiers in Iraq send emails and photos home. They also depend upon emerging IT-based systems that ensure their paychecks arrive when and where expected – something spouses of deployed Soldiers could not depend upon at the start of the war. As the Department continues down this transformational path, further benefits of the use of IT can be seen in real world application. Two such examples pertain to use of IT by ground forces in Iraq, and the stellar improvement in Air Tasking Orders since Desert Storm.

In the first example, the 1st Cavalry Division implemented a tactical networked capability, known as CAVNET, during their 2004-2005 deployment. CAVNET linked tactical units and allowed information to be shared and updated on a continual basis, greatly enhancing the situational awareness and effectiveness of the division. In one instance, due to its ability to enable instantaneous information sharing across the division, numerous lives were saved as newly discovered insurgent improvised explosive devices (IED) deployment tactics were communicated to all units via CAVNET.

The second example pertains to Air Tasking Orders (ATOs). An ATO matches targets, aircraft, and munitions for each set of missions conducted. The order must also coordinate the many supporting assets including fuel and refueling requirements, intercept and jamming capabilities, and both ground and air tracking of hostile forces. In 1991, in Operation Desert Storm, an Air Tasking Order took 72 hours to produce, consisted of over 18 inches of paper, and had to be flown to ships and bases for hand-delivery. Changes required days of work – and delay. Today, ATOs are sent and received completely electronically, can be turned on 24 hour cycles, and are updated in hours, not days. Efforts are underway to develop a continuous planning and update capability, enabled by a net-centric environment that can more closely follow the dynamics of ongoing operations, and thus further minimize ATO timelines.

Transformation hinges on the recognition that effective access to and use of information is an incredible force multiplier and is critical to maintaining an advantage over adversaries in the current asymmetric threat environment. Smart leveraging of information allows decision makers at all levels to have early situational awareness for making better decisions faster and act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is at the heart of the capability required to conduct Network-Centric Operations (NCO) a construct that requires people, processes, and technology to work together to enable timely access to information, sharing of information, and collaboration among all involved. Instead of "pushing information out" based on individually engineered and predetermined interfaces, Net-Centricity ensures that a user at any level, whether a previously anticipated partner or an unanticipated addition to a coalition, can both "take what he needs" and "contribute what he knows."

As the National Defense Strategy points out, transforming to a network-centric force requires more than just implementation of IT capabilities alone. Achieving the full potential of network-centric operations requires viewing information both as a strategic asset and as a weapon system to be employed in all phases of the Department's missions

– and it requires fundamental changes in processes, policy, and culture of the Department as a whole.

Net-centricity, rooted in the cyber world, tends to be described in technical terms; but in reality, the concept is quite simple – Net-centricity connects people with information. To the men and women at all levels across the Services, it means, “I can get the information I need, where I need it and how I need it.” Net-centricity will enable distributed, integrated operations not only among the combat forces, but also across all the functions of the Department that provide combat power, such as logistics, medical, and intelligence, as well as provide it across all phases of planning, combat, post-combat, and peacetime. To achieve this vision, the legacy mantra to provide information on a need to know basis will be replaced by making information available on a need to share basis within a global information environment that will provide ubiquitous, assured access to information where and when the user needs it. This has been demonstrated in Afghanistan and Iraq where ground forces have been supported by Unmanned Aerial Vehicles (UAVs) that were flown remotely by pilots in Nevada. The Department’s investments in IT are key enablers to implementing this vision and improving the operational effectiveness of the warfighter and all defense operations.

Ensuring the delivery of critical capabilities that enable NCO is one of my major responsibilities as the DoD CIO. To further transformation, and in accordance with the National Military Strategy, we have undertaken the “creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations." We are doing this under the auspices of the Global Information Grid (GIG).

The GIG comprises the people, processes, and technology necessary to enable Net-Centric Operations. From the technological perspective, the GIG consists of: terrestrial, space, and wireless communications "***pipes***"; computing, processing, and storage "***machinery***;" ***enterprise services*** (such as Messaging, Discovery, and Mediation); and ***applications*** (both Joint and user-defined). These components, while under disparate network management and information assurance practices today will over time fall under federated enterprise systems management to provide end-to-end GIG performance monitoring and ubiquitous end-to-end Information Assurance (IA). Information access via the GIG will be enabled by implementation of a Net-Centric Data Strategy that is organized around Communities of Interest using a shared vocabulary to exchange information that ensures data are visible, accessible and understandable.

Information Assurance (IA) – protecting the data and defending the network – is as critical to the Department's Transformation as the GIG functionality described above. The importance of IA simply cannot be overemphasized, as evidenced by its selection as one of four Critical Joint Enablers considered in the Quadrennial Defense Review. In order to depend on the GIG as the transformational weapon system it has become, we must be confident the network will be there and trust the integrity of the data. To this end we have developed and are implementing the DoD Information Assurance Strategic Plan and the IA Component of the GIG Architecture as the overarching mechanisms to achieve and maintain the requisite level of assurance, a challenge that becomes more complex as the pace of technological change increases. The Department is also aggressively pursuing an Enterprise Architecture and prioritized enterprise IA solutions through centralized funding. These solutions include enterprise network defense tools to: automatically identify and detect anomalies; remediate software vulnerabilities; eliminate spy-ware and mitigate insider threats.

What other types of enterprise capabilities are we working to provide via the GIG? Some current examples of Joint capabilities to be networked include the following that are today contributing to Operation Iraqi Freedom (OIF):

- The Air Force's Global hawk (Unmanned Air System) is an example of an Information Technology platform that is providing daily intelligence, surveillance and reconnaissance support to the Global War on Terrorism (GWOT) in OIF.
- Global Command and Control System (GCCS)-Joint provides the means for the joint warfighter to plan, execute, and manage military operations. It is fielded and being used in OIF. It enables National Military Command Center (NMCC), Combatant Commanders (CC), Joint Force Commanders, and Service Component Commanders to plan and conduct military operations, and to maintain awareness of the battlefield. Commanders can synchronize air,

land, sea, space, and special operations forces using an identical view of the battlefield.

- Global Combat Support System (GCSS) - Combatant Commander/Joint Task Force is also being used in OIF. It uses the GIG to provide combat support data (predominantly logistics info) to the Commanders on the front lines, and it improves communications between forward deployed units and the sustaining bases.
- Blue Force Tracking devices have received wide acclaim by the Commanders in OIF. These devices provide Commanders up-to-date location information on deployed forces. In some cases it provides readiness information as well, so Commanders can determine the ability of units to participate in planned operations. These devices use a mix of Army developed and commercial products and use tactical terrestrial networks or commercial satellite communications to pass data to higher echelons. In support of OIF, the Armed Forces Health Longitudinal Technology Application, as part of the Theater Medical Information Program (TMIP), is currently deployed to medical units in Iraq and Kuwait. TMIP integrates components of various medical information systems to ensure timely, interoperable medical support for rapid mobilization, deployment, and sustainment of all theater forces anytime, in support of any mission, to protect combat power worldwide.

There are many IT efforts underway that will further the warfighter's and DoD's ability to win the long war and improve and continue to optimize its enterprise operations. One such effort is Net-Enabled Command Capability (NECC), formerly the Joint Command and Control (JC2) System. NECC will be the DoD enterprise C2 information technology. It will enable decision superiority via advanced collaborative information sharing achieved through vertical and horizontal interoperability. The current GCCS Family of Systems will migrate to NECC to provide force-level planning, execution, monitoring, and assessment of joint and multinational operations. NECC will use Net-Centric Enterprise Services and other enterprise services to exchange data cross multiple security domains.

In my role as the DoD CIO, I have a number of responsibilities in the acquisition process, which allow me to ensure that IT investments are meeting established cost, schedule and performance thresholds. I chair the Information Technology Acquisition Board and I am the Milestone Decision Authority (MDA) for major Information Technology acquisition programs in the areas of Command and Control, Communications, and such business areas as Health, Logistics, Procurement and Financial Management. As a member of the Defense Acquisition Board for weapon systems and the Defense Business System Management Committee, I am responsible for ensuring these systems are in compliance with IT policy. I also have responsibility for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance and IT acquisition policy and co-sign the Department's Acquisition Instruction (DoD Instruction 5000.2). We have incorporated, or are in the process of incorporating, into the acquisition instruction and guidance, policies and procedures in the areas of implementation of Title 40 (previously the Clinger-Cohen Act), net-centric operations, data management, spectrum management, the acquisition of commercial-off-the-shelf software and compliance with the Global Information Grid. Lieutenant General Croom, who is here with me today, will address the important role his Agency plays in IT Services, to include the Global Information Grid-Bandwidth Expansion (GIG-BE) program. GIG-BE is a highly successful program that upgrades the existing Defense Information System Network to a 100 percent fiber-optic backbone and increased information flow across the network by an order of magnitude – the program was implemented on schedule and below cost.

Another successful program is the Satellite Teleport, which is upgrading the telecommunications capabilities at selected Standardized Tactical Entry Point (STEP) sites. This program incrementally provides multi-band and multimedia satellite connectivity from deployed tactical command, control, communications, computers, and intelligence systems to fixed base locations world-wide via Defense Information System Network (DISN). Installation of key satellite communications terminals began in 2005 with completion expected in 2006.

Interoperability for sharing information with our interagency and coalition partners is critical to winning the long war. The implementation of the Command and Control Information Exchange Data Model (C2IEDM) enables the sharing of situational awareness across the battle space with our partners. For example, the Army has mandated use of C2IEDM as its standard and is fielding it in the next software version of the Maneuver Control System. Likewise, our North Atlantic Treaty Organization partners have adopted this data model as their standard. Future U.S. systems like the Joint Common Operational Picture Work Station will also use this data model.

Competition for the Department's Radio Frequency (RF) Spectrum to satisfy new requirements and the commercial marketplace is a major challenge. The complexity of managing the RF Spectrum environment has caused the Department to significantly increase its oversight of this critical finite resource. New technologies, to include Counter-Improvised Explosive Device (C-IED), wireless systems, Global Positioning System are dependent on the availability of RF Spectrum. The Department has embarked upon upgrading the career progression of spectrum managers and the specialized training required to develop a cadre of experienced RF spectrum professionals that is so desperately needed by the warfighter in the theater of operation.

Information and Communications Technology (ICT) is an essential element of security cooperation and stability. The Department has bilateral agreements for sharing IT assurance data with other nations. The Department has also established the Regional International Outreach (RIO) program that provides a network web-based environment for open exchange of ideas, collaboration, distance learning, and information sharing that allows both international and national students, alumni and faculty to continue their education and discuss matters that pertain to: terrorism; internal and regional instability jeopardizing the territorial integrity of nation states; regional and local crises that could evolve into transnational threats or spur transnational terrorism.

In summary, information technology is critical to maintaining the strategic and tactical edge on the battlefield and to achieving many of the transformational capabilities that will keep our men and women out of harms way in the increasingly dangerous world we face. My job is to ensure that our investments in IT satisfy the warfighters' and users' requirements in a fiscally constrained environment.

I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.