NOT FOR PUBLICATION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

# STATEMENT BY

**THE HONORABLE**
**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**

***DEFENSE INFORMATION TECHNOLOGY***

**MARCH 28, 2007**

**NOT FOR PUBLICATION**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

## Introduction

Good afternoon Chairman Smith, Congressman Thornberry 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 overall missions of the Department of Defense (DoD). I am John Grimes, the Assistant Secretary of Defense for Networks and Information Integration and the Department's Chief Information Officer (CIO). My statement will focus on how the Department is leveraging information and information technology (IT) to rapidly respond to unpredictable, unanticipated and unknown global national security challenges of today and tomorrow.

The 2006 Quadrennial Defense Review (QDR) states that achieving net-centricity is critical to "harnessing the power of information connectivity." As we move forward to support the Department's Transformation and the QDR goals, the focus of net-centric operations and activities is ***to provide a more effective and efficient force***. That "force" includes the warfighter, the intelligence community and the business processes that support and enable the warfighters' success. Regardless of time or place, each different element of the force must be able to say, "I can get the information I need to perform my mission," and our transformation efforts are focused on enabling that.

## Net-Centric Operations

The ability to access information, to share the information and collaborate with others is at the heart of net-centric operations. To make this happen, we have established four fundamental goals—to effectively build, populate, operate and protect the information network. To '***build***' and modernize our network, we must ensure that the latest technology and infrastructure is available so that the warfighter can operate in a speed-of-light information world. To effectively ***populate*** our network with critical and timely information, we must provide the mechanisms by which data can be posted or stored and readily accessed by users. To ***operate our*** enterprise network we must ensure that data is accessible, reliable and available whenever and wherever it is needed, while at the same time ***protecting*** our network against an adversary who is determined to exploit the cyberspace arena.

The ongoing transformation represents a fundamental change – that is, a change in both what is being done and how it is being accomplished. This strategy requires a cultural shift regarding how information and IT are viewed and used.

## Information Stewards, Not Owners

Today, there is enormous cultural reluctance to share information with others outside a particular community. Information is considered power, and power is not something to be yielded freely. Information is typically stored in bins and silos that are walled off from those who feel they "own" the information and data. This "need to know" culture is shifting so that we place greater emphasis on understanding who else would benefit by making information accessible. The importance of "need to share" and, more importantly, "right to know" must be recognized. An authorized user, in essence, has the ***right*** to access information that is critical to doing his or her job and in today's information environment we have the technology to provide this capability securely.

To help realize this vision of information sharing, the Department's Data Strategy and Communities of Interest (COI) concentrate on realizing the principles that data must be visible, accessible, and understandable to authorized users. To do so requires "tagging" of data with discovery metadata and enterprise-wide services to enable information to be discovered and exchanged by users (human and machine) as a service within the Global Information Grid (GIG). To enhance the sharing of information among and between military, federal, state, local, private organizations and coalition partners, COIs are forming across a wide variety of functional domains which allow better exchange of information.

The recent overwhelming success of the Federal Maritime Domain Awareness (MDA) Data Sharing Community of Interest Pilot demonstrates how several executive branch agencies can leverage the early capabilities of the managed services provided by the Department's Net-Centric Enterprise Services (NCES) program to effectively and efficiently share mission critical information. This pilot included the discovery and machine-to-machine sharing of maritime vessel identification, location, speed, course, and destination information among the Navy, the Department of Homeland Security (DHS), the Department of Transportation (DoT) and the Office of Naval Intelligence. The MDA effort also made use of a Google-like federated search capability to advertise, discover, publish, and subscribe to unclassified maritime vessel tracking data. The MDA pilot provided three Federal Departments (DoD, DHS, and DoT) daily access to over 5,000 maritime vessel tracks they previously did not have, and enabled analysts and law enforcement officials to rapidly exploit the new information to better secure our coasts, ports, and waterways. This important net-centric operations capability was delivered in nine months for approximately $1.3 million.

In close cooperation with the Director of National Intelligence (DNI) CIO we are developing a standard, that is, a core vocabulary and data representation, for concepts such as "what," "when," and "where" that are universally understood across the many mission areas of the DoD and the Intelligence Community (IC). These standards are being applied as the basis for the Strike Community of Interest, led by United States Strategic Command, and will enable the multiple agencies and Military Services within that Community of Interest to share and understand critical mission data. The Strike Community is focused on the delivery of joint net-centric command and control and coalition strike planning capabilities that include assets from the IC. Interagency cooperation between DoD and the IC is essential for sharing critical counter-terrorism and intelligence information among the national leadership, the war planner, warfighter and combat support elements.

## Information Enterprise, Not Information Stovepipes

Much of today's information environment is still characterized by stovepipes and systems in which information is, quite frankly, hidden and hoarded, rather than visible and shared. Additionally, many of our existing IT systems cannot talk to each other without the benefit of time-consuming, costly, pre-engineered interfaces. Solutions are based on predetermined needs despite the fact that in today's world it is not possible to anticipate what will be needed or by whom. The challenge is to design, engineer, and create an information environment that can adapt to new users, new technologies and new challenges, rather than one which is static and emphasizes platforms and systems alone. Enterprise services and net-centric solutions are the only way we can overcome these legacy inefficiencies.

To ensure interoperability with legacy systems and ensure end-to-end performance, we are applying extensive enterprise-wide system engineering early in the requirements and decision process. We have established an enterprise-wide systems engineering capability to provide the mechanism by which the Department can collaboratively develop technical interoperability and performance solutions that fosters a truly federated information environment.

## Framework for the Future, Not Grand Design

Today's information systems have been developed to retrieve and manipulate data according to very specific and highly tailored requirements. Each organization tends to pursue its own needs.  The result has been a multitude of systems that not only cannot communicate with each other, but are often proprietary, not easily modified and not readily transferable to other needs.  To remedy this, we are moving toward enterprise level, end-to-end, lifecycle management of how we design systems and deliver services to the warfighter.

The Department is moving away from a "grand design" systems approach as the basis for its information environment and instead adopting Services Oriented Architecture (SOA) as the key to transforming to net-centric operations.  SOA supports an information environment built upon loosely coupled, reusable, standards-based services.  It promotes data interoperability rather than application interoperability.  SOA ensures providers can reuse what already exists, that is, pieces of applications and data, rather than recreating them each and every time.  Moreover, it allows new capabilities to be delivered more quickly.  It is allowing the Department to separate data from applications for sharing information within and across the Enterprise Information Environment (EIE).

The second key to success in this area is using commercially managed network services. The Defense EIE will provide commonly available core services; that is, services commonly needed by a wide range of users.  Services are required to access, manipulate, share data, and, most importantly, to collaborate across the enterprise.  Such core network services must be viewed as resources to manage, rather than applications to be owned.  A crucial IT investment for making this a reality is the Department's Net-Centric Enterprise Services (NCES) program, being implemented by the Defense Information Systems Agency.  The first managed service, collaboration tools, has been verified and deployed. LtGen Croom will describe in more detail NCES and managed services in his testimony.

## Managing Investments by Portfolios, Not Programs

As a result of the 2006 QDR recommendations, the Department is moving to portfolio management, which provides improved management of IT, and other defense resources by ensuring that programs supporting the same capability portfolio are synchronized and that any duplication is eliminated.

For example, the Department has established four Capability Portfolio Management (CPM) pilots with the intent of managing groups of like capabilities across the enterprise to improve interoperability, minimize capability redundancies and gaps, and maximize capability effectiveness. This process is allowing the Department to shift to an outcome-focused model that measures progress by outcomes. The process offers the ability to look at the whole, rather than struggle to determine if there should be a connection between the piece parts. One of the four pilots is the Joint Net-Centric Operations (JNO) capability area, for which I am responsible.

## DoD FY08 Information Technology Highlights

As the Department's CIO, I set the policies for the Department's IT initiatives and investments, and I am the milestone decision authority for most of the DoD's major IT investments. Also, my office collects and reviews the Department's IT budget justifications which are ultimately submitted to OMB and Congress. The President's FY 2008 Defense budget request of $481.4 billion represents an eleven percent (11%) increase from what was enacted last year ($432.4 billion), while the Department's FY 2008 IT budget request of $31.5 billion reflects a three percent (3%) increase from what was enacted last year ($30.5 billion). Even though the overall Defense budget has increased due to wartime demands, the IT budget has remained relatively stable. It is critical that we maintain the funding levels requested in the President's Budget to implement successfully our strategic approach, and progress toward fully net-centric capability that will serve our warfighter and the Department’s business functions.

What are we buying with this $31.5 billion?

- Approximately $15 billion in communications and computing infrastructure – including programs such as the Defense Information System Network (DISN), Net-Centric Enterprise Services (NCES), Mounted Battle Command on the Move Program, base-level communications support and infrastructure, and Navy/Marine Corps Intranet (N/MCI);
- Just over $8 billion on warfighting and related national security information systems – including the Joint Tactical Radio System (JTRS), Global Command and Control System (GCCS), Net-Enabled Command Capability (NECC), Forward Area Air Defense Command and Control System (FAADC2), and Mission Planning System;
- Approximately $5 billion in business systems – including the Defense Integrated Military Human Resources System, Navy Enterprise Resource Planning, Defense Travel System, and other Defense Business Transformation efforts;
- Approximately $2.5 billion on Information Assurance initiatives to protect our networks and train our IA workforce; and
- Almost $1 billion on related technical activities such as transition to IPV6, developing technical architectures, and radio frequency spectrum management support.

## Defense Acquisition Transformation

Earlier this month the Department provided Congress with our first report on the Department’s ongoing Acquisition Transformation initiatives and the goals that we have established to achieve change.  The full report is available at http://www.govexec.com/pdfs/DATR_march7.pdf.  The report describes how the Department of Defense is aggressively transforming its institutional acquisition processes and systems to align with 21st Century national security and defense objectives, and achieve a more integrated, cohesive environment.  Every aspect of how we do business is being assessed and streamlined to deliver improved capabilities to our warfighters and to provide visibility to our senior leadership.  A significant part of this effort entails integrating capability, analysis, and resource processes with periodic review by the Department's Deputy's Advisory Working Group – the DAWG.

Early collaboration on investment decisions among the joint warfighter, acquisition, sustainment, and resource communities is being accomplished through common databases, analytic methods, lifecycle metrics, and networked information sources.  This level of in-depth collaboration is new and includes defining requirements in terms of effects-based outcomes and mapping resources according to "joint capability" areas.

## IT Acquisition – Initiatives and Accomplishments

We continue to address ways to improve the IT acquisition management and procurement processes that serve as examples of how we are actually transforming the way we do business and delivering net-centric capabilities.  These initiatives are aimed at improving results, saving time, and saving money while getting the capabilities, IT services and products in our customers' hands in a timely manner.

We are changing our approach and revising our acquisition model for IT to meet our goal of providing products to our customers, the warfighter, as quickly as possible.  Our new process is designed to improve cycle time of our IT acquisitions without losing the discipline of our current process.  We are adopting a Time Certain Development process that places a higher priority on schedule than in the past.  We will require our IT programs to change their focus on delivering useful military capability within specified periods of time. To enable this shift we will concentrate on developing and delivering smaller increments of technology within the broader program. These smaller increments will place a higher priority on lower risk, more mature technology. Using this approach, higher risk, less mature technology may be rephased to later increments in the program.

Improving cycle time is key to our new approach. We must also ensure that the operators of the new products are fully trained and that the users have a support infrastructure to rely on when additional help or replacement products are necessary.

Two additional improvement initiatives, risk-based source selection and incentive contract arrangements show a lot of promise. The objective of risk-based source selection is to provide an informed basis for assessing industry proposals, quantifying the risk in terms of time and cost, and enabling more informed discussions with offerors. The results will be more reliable estimates of program lifecycle costs, proposal risk, and improved management and stability.

The use of incentive arrangements in contracts provides motivation for excellence in such areas as quality, schedule, technical performance and cost management. In particular, award fee arrangements are often used when the nature of the work to be performed offers a wide range of potential outcomes, many of which may be beyond the contractor’s control. In view of these uncertainties, award fee arrangements are used to motivate the contractor in ways that will result in the best possible outcomes under the circumstances.

Also, the Department is changing the way we procure information technology. These include the DoD Enterprise Software Initiative (DoD ESI), and the federal SmartBUY Program, which is led by the Office of Management and Budget (OMB) and managed by the General Services Administration. Both initiatives seek to establish strategic relationships with key vendors, initially by consolidating the purchasing power of the

DoD and/or the other federal agencies to obtain optimal pricing and preferred terms and conditions for widely used commercial software and related services.  The SmartBUY Program often leverages existing DoD ESI resources, including software product management and contracting support, to establish “co-branded” SmartBUY/ESI agreements for use by the entire federal government.

The DoD ESI was established in 1998 to implement a software enterprise management process within the DoD.  As an ongoing joint, cooperative venture actively involving 10 separate DoD Components, the DoD ESI started by pooling commercial software requirements to present a single negotiating position to leading software vendors. Twenty-three software best practices were adopted by the DoD ESI Working Group, leading toward a DoD-wide business process for acquiring, distributing and managing Enterprise Software.  The DoD ESI has since expanded to include commercial software implementation services from major systems integrators, and information technology (IT) hardware.  Agreements are now in place with 37 major commercial software publishers and service providers, yielding substantial (approximately $2.5 billion) cost avoidance for DoD ESI customers .  Preliminary work will soon begin on an IT Asset Management Pilot to improve visibility of the commercial software and hardware that comprise a vital portion of the DoD’s capabilities.  DoD ESI leaders are members of the DoD Strategic Sourcing Directors Board, and contribute to the DoD Strategic Sourcing Report, submitted annually to OMB.

## Information Assurance

Information Assurance (IA) – protecting the data and defending the network – is as critical to the Department's Transformation as the data strategy described earlier.  The importance of IA to protect the information and infrastructure simply cannot be overemphasized, as evidenced by its selection as one of four Critical Joint Enablers considered in the QDR.

In order to depend on the GIG as the transformational weapon system it has become, we must be confident that the network will be available and we must trust the integrity of the data. To this end, we continue to follow the tenets of the DoD Information Assurance Strategic Plan and emphasize IA policy and systems engineering integration of complex IA capabilities. By doing so the Department ensures IA is implemented and managed across the enterprise in a standardized manner to enhance warfighter and business operations. I would like to highlight six initiatives that are helping to defend the GIG.

- First, we successfully piloted a commercial tool suite with integrated security solutions that will be installed on every computer and server in the DoD beginning in FY 2008. This suite monitors and blocks intrusions at the host level and will be centrally managed at the military service and agency level.

- Second, we are embarking on innovative ways to manage, train, and educate critical IA personnel in the Department. The IA Workforce Improvement Program (IA WIP) establishes specific Department level training, certification, and tracking requirements that Combatant Commands, Services, and Agencies must follow to train and certify the over 70,000 DoD IA workforce members to a common baseline standard.

- Third, I established a priority within my organization to provide technical and non-technical advice on the safeguarding of identities and sensitive information that characterizes people, systems, and services. The Department's identity management approach is composed of three technology-based programs (Public Key Infrastructure, Common Access Card, and Biometrics), which are used to ensure that identities for all entities (humans, devices, and applications) have been successfully authenticated and are properly managed and protected. This, in turn, increases the reliability and trust of the information provided, and most importantly, increases the overall safety of our warfighters.

- Fourth, my office, in conjunction with the DNI CIO, established the Unified Cross Domain Management Office in order to allow the DoD and Intelligence Community to more effectively share information between security domains—that is, to move information between networks at different classification levels throughout the federal government. This effort and associated technology are important because they govern the ability of federal intelligence agencies to inform state, local and tribal first responders about pending terrorist threats and it, enables information sharing among allies, coalition and other partners.

- Fifth, the Joint Task Force - Global Network Operations (JTF-GNO) continues to conduct an aggressive network defense campaign against growing threats to the Global Information Grid (GIG) by identifying significant threats and developing, disseminating and implementing countermeasures to these threats. LtGen Croom will describe in more detail the activities of the JTF-GNO in his testimony.

- Lastly, we continue to transform IA for the GIG through advanced research. DoD is researching techniques that will help the JTF-GNO to identify more rapidly and react to malicious activities. NSA continues to work on delivering a trusted platform to be used throughout the GIG, and researching secure, high-speed, optical switching techniques.

## IT Workforce

One final area I would like to emphasize is our workforce, which is critical to the implementing the net-centric vision and our goals. We are partnered with the

Information Resources Management College (IRMC) of the National Defense University to develop graduate level curricula and programs to meet current and emerging information technology management skills requirements for middle to senior level military and civilian managers within the Department. The curriculum is dynamic and reflects the latest policies, best practices and legal requirements to manage complex IT initiatives, as well as courses in continuity of operations, disaster recovery, national security and military operations, and cyber attack and defense computer laboratory exercises. The programs available provide certificates in a variety of IT disciplines, including IA. Through flexible on-line distributed learning course offerings we are able to get DoD IT professionals certified across the country and while deployed, including in Iraq and Afghanistan.

We have also engaged with our own national agencies as well as with international partners to create a forum where IT problems can be explored and solutions shared. Students from over 20 nations have attended IRMC's Advanced Management Program in residence at Fort McNair. In addition, IRMC has formed international agreements to assist in tailored, IT educational capacity building projects in course development and faculty enrichment with coalition partners such as Bulgaria, Romania, and Singapore.

We continue to recruit talented IA and IT personnel through the very successful IA Scholarship Program. Last year we awarded 23 new IA scholarships to university students and provided grants to universities and colleges to improve their IA research and curriculums. We currently have 75 National Centers of Academic Excellence in Information Assurance Education located in 31 states and the District of Columbia. This is a real success story.

## Summary

By now it should be evident that information and IT are critical resources in every aspect of the Department’s operations. The net-centric operations transformation will enable the Department to be more effective and efficient. This will provide timely situational awareness that enables superior decision-making by our senior leaders and warfighters and allows them to get into the enemy’s decision cycle.

The Department will continue to use the DoD data strategy to improve its information / data sharing across a multitude of domains, ensure that its information is protected and networks defended and secure; and continue to transform the acquisition process so that we can provide the best capabilities and tools for our soldiers, sailors, airmen, marines and those who support our warfighters.

Mr. Chairman, and members of the Subcommittee, I thank you again for the opportunity to speak to you today. We greatly appreciate the support you have given us, and I look forward to our continued collaboration. I would be happy to answer any questions you may have about the Department’s information technology initiatives.