WRITTEN STATEMENT OF

LIEUTENANT GENERAL CHARLES E. CROOM, JR., U.S. AIR FORCE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

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

THURSDAY
6 APRIL 2006

06-C-0585

Good afternoon, Mr. Chairman (Cong. Saxton), and Members of the Subcommittee. I am Lieutenant General Charlie Croom, the Director of the Defense Information Systems Agency (DISA) and the Commander of the Joint Task Force - Global Network Operations (JTF-GNO). I am pleased to appear before the Subcommittee today to discuss that portion of the Defense Department information technology budget which funds the Defense Information Systems Agency (DISA) and which the most recent Quadrennial Defense Review highlights as essential to achieving our goals relating to net-centricity and information assurance.

Across the Department of Defense, requirements supporting a global, interconnected force demand a transformation in the way information is managed and shared to accelerate decision-making, improve warfighting, create intelligence advantages, and optimize business processes. Net-centricity is the means by which we will accomplish this. The foundation is the Global Information Grid (GIG), which is the global end-to-end set of information capabilities and services for collecting, processing, storing, disseminating and managing information on demand for the Department.

As stated by the Assistant Secretary of Defense for Networks and Information Integration, net-centricity has three goals:

Goal #1 - Make information available on a network that people depend on and trust.

Goal #2 - Populate the network with new, dynamic sources of information to defeat the enemy.

Goal #3 - Deny the enemy comparable advantages and exploit weaknesses.

The essence of net-centricity is placing intelligence, command and control, logistics and business information in the hands of users, allowing them to plug in to the "network" from wherever they are and pull the information they need for their particular mission. Net-centricity will facilitate powerful, immediate decision making based upon machine-to-machine interaction wherever possible.

The Defense Information Systems Agency (DISA) has a crucial role in moving the Department toward net-centricity. We imagine and envision a world in which information is virtual and on demand with global reach. Information is protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner. It is a world in which United States military forces can deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. It is a world with well-developed and available standards and no seams between the sustaining base and the tactical edge that is enabled by an equally well-developed and available set of standards facilitating the exchange of data. It is a world in which services are converged and computing is done on a well-developed and available Internet Protocol (IP) network. It is a world in which the United States military can freely exchange information routinely with coalition partners and others responsible for the security and defense of the United States. The technology employed is agile, adaptive, and capabilities-based. It uses machine-to-machine communication and wireless connectivity, allowing connection regardless of location. And, we imagine and envision a world in which our soldiers, sailors, airmen, and marines are equipped with capabilities and services that are state-of-the-art.

To achieve net-centricity, the Defense Department's Global Information Grid will be a www-like enterprise in which people can discover information, orchestrate their own operational picture based on the situation at hand, and operate securely in a trusted manner. We will allow advanced networking technology and speed to bring people together efficiently, help them do their jobs in ways never anticipated, and enable them to mash services together to compose services to do things never envisioned. We have several challenges.

We need an infrastructure that ensures sufficient bandwidth, computing, and that storage is available and dynamically allocated to process and deliver information from edge-to-edge. This infrastructure includes a common assured communications network, with sufficient bandwidth consisting of terrestrial and non-terrestrial components.

We need a data strategy that enables information sharing and advances the Department from defining interoperability through point-to-point interfaces to enabling the "many-to-many" exchanges typical of an interconnected environment. Data must be an enterprise asset that is visible, available, usable, and trusted on the network when and where needed.

We need the capability to link producers of information and consumers of information. This will be enabled by a set of core enterprise services that include discovery, mediation, and security.

We must command and control the network and aggressively defend it. I will address information assurance toward the end of my testimony.

And, finally, we must have a capabilities-based approach to acquisition moving away from the traditional system and program-centric manner in which the Department acquires today. And, we must be able to acquire information technology capabilities and services at near Internet speed to put them in the hands of our warfighters such that they have the advantage over our enemies. We will strive to increase the speed and flexibility of the processes we have employed for decades in acquiring capabilities and services, and we will strive to tailor oversight and governance to be commensurate with risk. We will accelerate acquiring services and capabilities to close the gap between the availability of technologies and fielding them for warfighting advantage.

The Defense Information Systems Agency (DISA) will follow the precepts of adopt before we buy and buy before we create. If another agency of the Department has developed or acquired a solution that either fits or is close to fitting a need we have, we will adopt it. Failing the opportunity to adopt from within the federal government, we will turn to the private sector and adopt a managed service that either fits or is close to fitting the need. In both cases, we will do a risk analysis to determine if we can realistically use something that delivers less than 100 percent of the need, what elements will not be satisfied, and whether or not they are so crucial so as to preclude adopting either the other government solution or the managed service. We will also determine if a second or third source can be used to provide the critical missing elements and if that course of action is feasible and cost effective. The final choice is to create or build a solution. We intend to avoid development and turn to others for solutions when we can.

The pursuit of net-centricity has resulted in the evolution of a number of programs for which the Defense Information Systems Agency is responsible. They include the Global Information Grid Bandwidth Expansion (GIG-BE), Net-Centric Enterprise Services (NCES), and Network Enabled Command Capability (NECC), formerly called Joint Command and Control (JC2).

The Global Information Grid Bandwidth Expansion (GIG-BE) reached full operational capability at the end of last year, and is deployed to 85 sites globally. It provides significantly increased bandwidth that is highly scalable to meet the Department's most critical command and control and intelligence surveillance and reconnaissance needs. It provides physical diversity, redundancy, and automatic traffic rerouting to ensure the reliability and robustness of communications to critical locations. It was built to meet the most exacting security standards of both the Department and the intelligence community, and it has been accredited for processing sensitive but unclassified, secret, and top secret sensitive compartmentalized information. We were able to accomplish this by using innovative contracting techniques and partnerships with industry experts to acquire, engineer, integrate, and test state of the art commercial components and technologies. It is the terrestrial component of the Department's transformational goal to remove bandwidth as a constraint.

The Global Information Grid Bandwidth Expansion (GIG-BE) was designed to service not only the Department's fixed installations, but also to extend transformational communications to deployed warfighters by connecting to another Defense Information Systems Agency (DISA) provided capability, the Teleports. Connected to the Global Information Grid Bandwidth

Expansion (GIG-BE), Teleports provide warfighters deployed anywhere in the world secure and interoperable communications through military and commercial satellite communications.

The Global Information Grid Bandwidth Expansion (GIG-BE) is being integrated with the Department's existing communications network, the Defense Information Systems Network (DISN). Together, the Global Information Grid Bandwidth Expansion (GIG-BE), Teleport, and the Defense Information Systems Network (DISN) provide a single, integrated network that delivers secure net-centric communications to the entire spectrum of Department of Defense (DoD) users as well as our Intelligence Community partners.

Net-Centric Enterprise Services (NCES) will provide the core services that will allow users and systems to find and access relevant information on the network. It will allow users to make information they produce available for others to discover. And it will allow collaboration in a more effective manner.

Net-Centric Enterprise Services (NCES) defines the role of both the consumer of a service and the services themselves in the Department's Internet-like environment. The consumer who has a need for information can search to locate a service that provides the information and can determine the context of its use, without concern for how the need is filled. The service providing the information can be found in a registry, fills the need, and is reusable.

Net-Centric Enterprise Services (NCES) has four product lines that offer a variety of these services. The collaboration product line includes web conferencing and instant messaging along with a number of other commonly available collaboration tools. Content discovery and delivery

will provide a federated search service, an enterprise catalog service, and delivery of content to the edge. The portal will provide user access to all the services.

The heart of Net-Centric Enterprise Services (NCES), though, is the service oriented architecture (SOA) foundation. This will provide the behind the scenes machine-to-machine services that allow the rapid and sure sharing of information. These services include security, mediation, discovery, and other "behind the glass" services that will make the Department's enterprise function in a manner similar to the way services are provided on the Internet. The idea behind a service oriented architecture is that each function in a business process is placed somewhere on the network and is built and maintained by the organization most capable of providing the function. The function is then provided as a *service* to other people and machines on the network. A business process or a mission thread is constructed by combining many different services together.

An example of a service might be a mapping service that would provide a map of a particular region of the world when asked. A command and control capability built around a service oriented architecture might use such a mapping service and combine it with a blue force and red force tracking service to produce a map with the positions of good guys and bad guys on it. The mapping and tracking services could evolve more or less independently of each other and the consumer of the command and control service would immediately benefit from improvements in either. This loose coupling of services is in contrast to the tightly coupled software development approaches we have traditionally employed. In addition to allowing easier evolution of the underlying services, the service oriented architecture also allows more information to be exposed

as a service, and allows services to be hooked together easily in new ways and allows the fast construction of novel and innovative business processes.

The Network Enabled Command Capability (NECC) will provide agile command and control capabilities supporting a high operations tempo and decision-making. It will be based on the service oriented architecture foundation and on net-centric collaborative information sharing and web services provided by the NCES program.

It represents the evolution from the highly successful Global Command and Control System (GCCS) to an Internet-like series of capabilities. It will move the Department from multiple architectures to a single service oriented architecture framework, and from multiple acquisition structures and decision makers to a single acquisition structure and milestone decision authority. The Network Enabled Command Capability (NECC) will shift us from the concept of a prescriptive common operating environment to the use of core enterprise services that are tailorable to the mission or need at hand. Said differently, it will move us from a pre-defined common operational picture and reports we have today to a user defined operational picture based on the user's particular needs and circumstances at the time.

A fundamental element of our approach to Network Enabled Command Capability (NECC) is teamwork with stakeholders, customers, and vendor partners. We will use a federated development and certification environment (FDCE) in which all can participate to foster innovation and collaboration and to introduce new services and capabilities into the Global Information Grid (GIG). We will ask customers to play in the "sandbox" by exposing candidate

capabilities and services (core, command and control, and business) to the FDCE and to warfighting and business users. We will incentivize vendors to do the same. Some candidates will take off; some will not. Our success will be dependent in part on our ability to do an early kill of those that do not. In any case, this richly collaborative approach will bring the best and brightest to the forefront and help us to speed the delivery of capabilities and services to warfighters.

The Global Command and Control System - Joint (GCCS-J) is the Department of Defense's current joint system of record for providing the command and control tools necessary to ensure decision superiority and battle space awareness. We have released 48 upgrades for the Global Command and Control System - Joint (GCCS-J) since September 11, 2001 addressing operational and security requirements in support of Operation Enduring Freedom, Operation Iraqi Freedom, and Horn of Africa, and we have done this without any mission disruption. Some have likened this to changing the tires on a car moving at 80 miles per hour. And, we are leveraging technology to efficiently and effectively tailor the Global Command and Control System - Joint (GCCS-J) to a web-based service oriented architecture, laying the foundation for the Network Enabled Command Capability (NECC) effort.

The Global Combat Support System (GCSS) is the current system for automation of combat support. It enables interoperability between combat support and command and control functions, and it provides a seamless flow of operational and sustaining base information to the warfighter. It helps the warfighter requisition, deliver, and account for supplies and manage logistics. It is a

complement to Global Command and Control System - Joint (GCCS-J) and a natural evolution to Network Enabled Command Capability (NECC).

I would now like to talk about information assurance for the Global Information Grid (GIG).

As we make the transition to net-centricity, protection of the Department's ability to execute its mission in the face of a cyber attack becomes ever more important. The Defense Information Systems Agency (DISA) is responsible for planning and executing an important part of the department-wide strategy for information assurance. In addition, in my role as the commander of the Joint Task Force - Global Network Operations (JTF – GNO), I have day-to-day operational control of information assurance operations. Daily we take advantage of the synergy between these two organizations. For example, over the course of the last nine months The Defense Information Systems Agency (DISA) and the Joint Task Force - Global Network Operations (JTF – GNO) have coordinated in the development of a set of near-term actions to shore up defenses throughout the department. Then, as commander of the Joint Task Force - Global Network Operations (JTF – GNO), I directed that these actions be implemented throughout the global information grid. I will talk more about some of these near term actions later.

The Global Information Grid (GIG) crosses organizational boundaries inside and outside the Department of Defense (DoD). It is composed of a huge variety of computer, software, and communications technologies acquired by many different Department of Defense (DoD) entities. As the Department moves to net-centricity, an imperative is to assure missions that depend on

the Global Information Grid (GIG) work well, in spite of an adversary's attempt to disrupt them via cyber attack. Another imperative is to properly balance broad information sharing with secrecy. The military will always need to hold certain information closely. At the same time, we believe we need broader information sharing within the Department and with other federal, state, and local partners; allies; suppliers; and the public.

Our strategy for achieving the necessary mission assurance and the necessary safe sharing has several tenets. One is we must improve accountability for information access by using non-forgeable cyber identity credentials in much the same way we use physical identity cards to access bases and buildings. Another is we must deploy and operate a Department-wide layered defense scheme that uses complementary protections in ways that stop many attacks before they have an effect on mission accomplishment. The third is we must be able to detect and quickly respond to any attacks that may get through our defenses. Finally, we must develop and follow a single Departmental plan for the design, implementation, and operation of the information assurance necessary to achieve the other tenets.

We will eliminate anonymity by the broad use of globally meaningful identity as a means of improving *safe* sharing in the Global Information Grid (GIG) and with our partners. The identity strategy we are pursuing revolves around the issuance and the broad use of cyber identity credentials based on a technology called public key cryptography. The Defense Information Systems Agency (DISA) is partnered with the National Security Agency, the Defense Manpower Data Center, and with the Military Services to build and use a credential issuing and verification system called a public key infrastructure (PKI). The public key infrastructure (PKI) credentials

are generally issued on smart cards that are called common access cards (CAC). The common access card (CAC) is the newer version of the classic Department of Defense (DoD) identification card and is used as the physical access token for many bases and buildings throughout the Department. The cyber identity credential is issued at the same time the common access card (CAC) is issued. As a result, the Department now has both physical and cyber identity credentials that have a common meaning and a common level of credential quality across the entire Department.

Virtually everyone has a common access card (CAC), and smart card readers and software are now deployed throughout the Department. In addition, virtually all Department web servers have a public key identity credential that can be used to identify the server to other computers and to any web browser.

Now that the cyber identity credential is widely deployed, as the commander of the Joint Task Force-Global Network Operations (JTF-GNO), I have directed the common access card (CAC) and its associated cyber identity credential be used as the logon credential for all unclassified Department workstations. The immediate effect of this action is to greatly reduce the Department's vulnerability to certain attacks against passwords.

I have also directed that the cyber identity credential be used when accessing all internal department web servers. This action enables servers to easily verify that someone accessing the server has been issued a proper credential. This verification can be used to limit access only to those with the credential. Since every site requires the same cyber identity credential, we can

now tie a particular person to patterns of data access across multiple web sites. This means we can begin to look for patterns of misuse that were almost impossible to detect before. We expect to have small-scale misuse detection systems fielded and operating in fiscal year 2007, and as we gain experience with these we expect to scale them up in the following years.

The cyber identity credential becomes even more critical as the department moves to build its information systems around the service oriented architecture design approach. As I have mentioned before, the Department is moving toward this approach for many of the same reasons industry is moving in this direction.

The agility in data access, in the rapid construction of new warfighting processes, and in the enhanced collaboration of forces the service oriented architecture provides is one of the ways the Department is confronting the uncertainty of modern warfighting.

One of the tricks to building such a service oriented architecture, is finding a safe way for potentially thousands of services to be put on the network to interoperate with thousands of other services. The cyber identity credentials play a critical role here too. We will issue a credential to each service on the network. In a manner exactly analogous to the use of a cyber credential by a person, this machine credential can be used by one service to identify itself to another service somewhere else on the Global Information Grid (GIG). This allows us to construct common access control mechanisms for service-to-service and for person-to-service interactions, and also allows us to drive the same sort of global access accountability I described above.

As part of the Net-Centric Enterprise Services (NCES) program we are building a set of security services that will sit on the network like any other service in a service oriented architecture. These core security services will help other services in the Global Information Grid (GIG) do things like determine a cyber identity credential is valid or determine whether a particular person has access rights to a particular service.

Another part of the information assurance strategy for the movement to net-centricity involves designing and building a set of layered defenses. The layered defense strategy is straightforward, but complicated to execute in an infrastructure as large as the Global Information Grid (GIG). The layered strategy includes proper configuration and operation of every device in the Global Information Grid (GIG), in conjunction with the proper design and operation of several layers of perimeter defense.

The inner most defense is the computer itself. The efforts of the Defense Information Systems Agency (DISA) and the Joint Task Force-Global Network Operations (JTF-GNO) have provided processes that include the development of Department of Defense (DoD) standards for secure configuration of devices in the Global Information Grid (GIG), the deployment of these configurations to every component, the development and deployment of modified configurations, including patches, as new vulnerabilities and attacks are discovered and developed, and the local and global auditing and reporting of compliance with the configuration standards.

Ensuring each computer is configured securely and each stays configured securely as conditions change seems like a simple problem, but it has been a tough problem to solve for us and for

industry. Many factors contribute to the complexity of this goal and make it hard to achieve. These include the intricacies of configuring a modern operating system securely; the difficulty in knowing that once configured, it is configured correctly; the sheer volume of new vulnerabilities in many operating systems; the increasing numbers of systems that need to be maintained, and the difficulty in updating and verifying the security of each of these machines in response to each new vulnerability.

The first step is to determine the secure configuration for a particular operating system. We have had success with innovative government and industry partnerships in developing best practices in operating system and application configuration. These partnerships have resulted in consensus security configuration documents for many operating systems and other devices that are published by the Defense Information Systems Agency (DISA) and the National Security Agency as Security Technical Implementation Guides (STIGs). Some are also published by the National Institute of Standards and Technology. Commercial Microsoft Windows systems administration training is now available that teaches to the standards defined in these guides, and finally, some major computer vendors are shipping computers pre-installed with these configurations.

Another aide to the configuration of machines is the use of tools that automatically scan for vulnerabilities and configuration errors. The Defense Information Systems Agency (DISA) purchased a Department-wide license for a vulnerability scanning tool that is now available to every system administrator in the Department, along with training and other support. Now that we have such a tool available to everyone in the department, in my role as the Joint Task Force-

Global Network Operations (JTF-GNO) commander, I have directed the entire Department use such a scanning tool.

With the worldwide usage and sheer complexity of common operating systems and applications, developers, users, researchers, and adversaries frequently discover vulnerabilities. As each new vulnerability is identified, software vendors mount a rapid effort to understand the ramifications of the vulnerability and to develop a fix that removes or at least minimizes the vulnerability. Information about a new vulnerability often becomes widely known in a matter of days. Therefore, a critical component of configuration and vulnerability management is to keep operating systems and application configurations up-to-date with the latest vulnerability patches as they are released. The Joint Task Force-Global Network Operations (JTF-GNO) has implemented a process called the Information Assurance Vulnerability Alert (IAVA), process to mandate the application of these fixes for software and configurations when a significant threat exists. When I issue an alert from the Joint Task Force-Global Network Operations (JTF-GNO), the process requires the Combatant Commanders, Services, Defense Agencies, and Field Activities to immediately update configurations to incorporate the new patches or to take other vulnerability remediation actions, and to report their compliance so overall Department of Defense (DoD) risk can be determined by the Joint Task Force-Global Network Operations (JTF-GNO).

Application of patches and other configuration changes to many machines quickly is the crux of the vulnerability management problem. We have not fully solved this, but we have taken significant steps to make configuration change easier and more certain. Again, the Defense

Information Systems Agency (DISA) purchased a department-wide license, with appropriate training and support, for a patch management and configuration management tool that can reduce the complexity and greatly speed the deployment of patches and configuration. I have directed such a tool be used throughout the Department, and implementation will proceed through fiscal year 2007.

The Defense Information Systems Agency (DISA) has also established a distribution system for the dissemination of security relevant patches throughout the Department. Patch repositories and anti-virus distribution servers are available on the classified and unclassified networks. These repositories enhance our ability to protect against newly announced vulnerabilities because we are no longer competing with the entire Internet community for access to vendor-released patches. Department of Defense (DoD) users have exclusive access to the repositories, thus speeding up the overall response. From this foundation we have established on the unclassified and classified networks, DOD Software Update Service (SUS) Servers, for the Microsoft baselines. These Software Update Service (SUS) Servers provide Department of Defense (DoD) system administrators with automatic notification, and if desired, automated download of significant Microsoft security updates. We have ongoing efforts to improve these services by ensuring patch and antivirus servers are available in places with limited bandwidth, and by ensuring patches are available from vendors even though the Internet may be unavailable.

Several layers of perimeter defense typically protect computers in the Department. These help to limit the number of people and other computers that have access to a particular vulnerability, should one exist. The Defense Information Systems Agency (DISA) runs a department wide

community risk management process call "ports and protocols" that determines standard policy for what will transit these defenses. This process and policy are essential for ensuring both security and joint application interoperability.

A significant effort in fiscal year 2006 and 2007 is the strengthening of the outer perimeter of the Department. As the Joint Task Force-Global Network Operations (JTF-GNO) commander, I have directed all publicly facing or partner facing services and applications in the Department be hosted in cyber demilitarized zones (DMZs) that sit between the department and the outside world. This is very much in keeping with the way any large corporation shares information with those outside the corporation. As we do this, we will be able to do most of our interaction with partners via these demilitarized zones (DMZs).

Another important effort, in fiscal year 2006 and 2007, is the design and construction of a more capable attack sensing and diagnosis infrastructure. The Defense Information Systems Agency (DISA) is leading a department-wide effort to design such an infrastructure. Piloting and operation of some capabilities has begun, with much broader capability deployment beginning in fiscal 2007. This will give all of our network operations forces much better ability to react quickly and effectively to cyber attacks.

I would like to finish my testimony on our information assurance efforts by saying we are collaborating with the Office of the Assistant Secretary of Defense for Networks and Information Integration, the National Security Agency, and the Military Services to build and then execute a Department of Defense (DoD) wide plan for the execution of these and other initiatives.

Now let me discuss the importance of Spectrum as an enabler for Net-Centricity.

As the Department of Defense (DoD) transforms to net-centric warfighting concepts, the realization of a fully networked and highly mobile battlefield will be increasingly dependent on assured access to the radio spectrum. Consequently, the electromagnetic spectrum emerges as the dominant transmission medium for tactical mobile forces to move information effectively; and, integrate wireless systems into a cohesive part of the warfighting force.

Because of the net-centric vision to accommodate and interconnect people and systems independent of time, location, topology, and routing, planning complexity increases to a level such that current processes cannot adequately manage available spectrum.

Net-Centric Spectrum Management will provide spectrum support by assuring on-the-move access and interference-free operations. These assurances are the basic tenets of net-centric spectrum management and support achievement of the "ubiquitous, robust, trusted, protected network" envisioned by the Department of Defense (DoD) Chief Information Officer (CIO).

Because of the complexity of the mobile tactical environment, Spectrum Management must be decentralized and performed autonomously throughout the network to be successful. Achieving net-centric Spectrum Management will require active participation throughout the Department of Defense (DoD) and also require direct and continuous liaison with both national and international spectrum entities. Net-Centric Spectrum Management will not be achieved in the near future, but will evolve as systems, processes and practices assimilate the attributes of net-centricity. This will require continued refinement as net-centricity matures and will be amended and revised as necessary to assist in assuring the attainment of an operational net-centric environment. The Defense Information Systems Agency (DISA) is supporting two key

initiatives to achieve transparent spectrum access for net-centric operations in order to facilitate understanding of the relationships and dependencies among systems, data, information, materiel and services that enable them to operate effectively together: the Defense Spectrum Management Architecture and the Global Electromagnetic Spectrum Information System (GEMSIS).

Mr. Chairman, I believe that we have been highly successful in delivering command and control and combat support systems and their supporting information technology infrastructure. As we move further toward net-centricity, we have initiated programs that will deliver the communications, data processing, and security that will allow us to provide net-centric capabilities and services to our nation's warfighters.

Thank you.