Good afternoon, Mr. Chairman (Congressman Smith), Congressman Thornberry, 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).

Information is America's greatest weapon system. Rapidly sharing information to ensure the warfighter has the right information at the right place and time remains our goal. Therefore, across the Department of Defense and with our partners in the Information Sharing Environment (ISE), requirements supporting a global, interconnected force demand that we continue the 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 four goals:

- Build the net
- Populate the net
- Operate the net
- Protect the net

In pursuit of these goals, the Assistant Secretary has challenged us to accelerate the adoption of a net-centric culture in the Department, make information a force-multiplier, aggressively defend the network, facilitate warfighter connection to all information including intelligence information, achieve agility with non DoD partners, and invest in information technology prudently.

The essence of net-centricity is placing all information – 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. We view the network as one including communications, computing, and storage, all provided and managed in a coherent, dynamically scalable and secure manner. Net-centricity will facilitate powerful, immediate decision making based upon machine-to-machine interaction wherever possible.

To achieve net-centricity, the Global Information Grid must 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 must bring people together efficiently, help them do their jobs in ways never anticipated, and enable them to compose services to do things never envisioned.

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. It is enabled by an equally well-developed and available set of standards facilitating the exchange of data. It is a world in which information services, such as voice, data, and video are converged on a mature, technology-fresh, and available Internet Protocol (IP) network. It is a world in which the past differentiation between the network and computing or data processing no longer exists since computing will be done virtually across the entire 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. In addition, by partnering with the ISE, we can ensure the Global Information Grid

connects not only the defense and intelligence communities, but homeland security, foreign affairs, and law enforcement - all of our partners in the Global War on Terrorism. 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 Information Technologies capabilities and services that are state-of-the-art.

Frankly, achieving our goals is easier said than done. We have several challenges.

Supporting the network, we need an infrastructure that ensures sufficient bandwidth, computing, and storage are available and can be dynamically allocated to deliver information anywhere in the world as missions dictate. This means a global communications network, with sufficient terrestrial and non-terrestrial bandwidth, that can be configured, allocated, and managed end-to-end. If we are to provide this, it is no longer sufficient for components of the Defense Department to provide segments of the network that are independently engineered, acquired, and managed. DISA will work with the Military Services and Defense Agencies to bring coherence to the network. This will include adequate standards, enterprise-wide systems engineering, a common strategy for architecture, a single concept for network operations and configuration control, and situational awareness of the network from the sustaining base to the edge.

The DoD data strategy focuses on making much more information available, often as a service on the network, so that people who might need the information but previously could not get it, have access. It also aims to advance the Department from defining interoperability through point-to-point interfaces to enabling the “many-to-many” exchanges typical of an interconnected environment. The notion of unanticipated users having access to information means a change from a need-to-know access control model to a consumer-driven access control model. Our data must be an enterprise asset that is visible, available, usable, and trusted on the network when and where needed. We need to work diligently to ensure the data strategy is properly enforced.

We need the capability to link producers and consumers of information across all mission areas – warfighting, business, and intelligence. This will be enabled by a set of core enterprise services that include discovery, mediation, and security. Further, we are acquiring a new set of joint command and control capabilities, based on these core enterprise services, to provide warfighters the ability to define and share information specific to the mission at hand.

As another part of the data strategy implementation, certain kinds of software development in the department are embracing this notion of services-on-the-network. Many business processes will soon be constructed as a loosely-coupled composition of these network-based services. This sort of business process construction is called a *service-oriented-architecture* (or SOA), and we believe it will allow for the more rapid evolution of warfighting processes in the department.

We must command and control the network and aggressively defend it. I will address information assurance later on in my testimony.

We must have a capabilities-based approach to acquisition that moves us away from the traditional system and program-centric manner in which the Department acquires today. 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, and we will strive to tailor oversight and governance to be commensurate with risk. And, we will strive to close the gap between the availability of technologies and fielding them for warfighting advantage.

Our final challenge is paying for the advancements we need. Last year, we experienced two cuts from another Committee, a 26 percent cut in Research, Development, Test and Evaluation (RDT&E) in the Network Enabled Command Capability (NECC) and a 7.5%

cut in procurement for the core services provided by the Net-Centric Enterprise Services program. Frankly, those hurt our efforts.

As I mentioned earlier, DISA has as crucial role in providing the capabilities and services essential to net-centric operations and warfare. From my point of view, DISA has four pillars essential to the Department's mission. These are:

1. the underlying network, or the Defense Information Systems Network or DISN;
2. the computing infrastructure provided by our Defense Enterprise Computing Centers or DECCs;
3. the core enterprise services that enable and facilitate sharing information among systems and users;
4. and the programs that enable command and control, today the Global Command and Control System (GCCS) and that enable us to provide combat support information and management, Global Combat Support System (GCSS).

While both are evolving to becoming net-centric, they will be supplanted by the modern Net-Enabled Command Capability for joint warfighting, a truly net-centric, scalable set of capabilities and services which will be web-based and therefore proliferated far wider than the current client-server based GCCS and GCSS systems.

The evolution of the Defense Information Systems Network continues as we integrate the Global Information Grid Bandwidth Expansion (GIG-BE) capabilities into the network, a project I will describe in greater detail later in my testimony. The GIG-BE was delivered on time and within budget, the only one of the original transformational programs to do so. It is designed to service not only the Department's fixed installations, but also to extend transformational communications to deployed warfighters by connecting to another DISA-provided capability, the Teleports. Together, the Defense Information Systems Network, GIG-BE, and Teleport provide a single, integrated communications infrastructure, a key element in providing the virtual, "always on network" I referred to earlier. Just as you replace your personal computer, the Defense Information Systems

Network must replace obsolete technology which is no longer supported by vendors, and that costs money, a challenge the Department is addressing. The network must expand, and contract if need be, to meet changing demands in the world. The establishment of the Africa Command provides a good example of our changing network. This too costs money.

The computing infrastructure and our Defense Enterprise Computing Centers (DECCs) must continue to evolve as well. The private sector has turned to web-based, highly scalable computing platforms that enable businesses and you and I to compose services on demand to meet daily needs. So too must our computing infrastructure provide highly scalable, on-demand processing. However, we must also deal with disadvantaged and disconnected users. We continue to have bandwidth challenges at the tactical edge, and we will for the foreseeable future. We have warfighting units on the ground, at sea, and in the air that are by necessity at times disconnected from the network. Both of these conditions demand that we provide capabilities and services beyond connecting to the "cloud". We must enable disconnected use in bandwidth limited situations through content staging and delivery and solid end-to-end engineering and configuration control.

The pursuit of net-centricity has resulted in the evolution of a number of programs for which the DISA is responsible. They include the Net-Centric Enterprise Services (NCES), and Network Enabled Command Capability (NECC), formerly called Joint Command and Control (JC2).

To help speed the transition to the DoD data strategy and to the Service Oriented Architecture, DISA is developing Net-Centric Enterprise Services (NCES). NCES will provide a set of core services focused on information sharing, enabling data access and the construction of SOA -based business processes. Some of these services will help people find and understand information contained in the services on the network. In addition to these, NCES will provide standards and some core services aimed at enabling the consumer-driven access control I described above. Service consumers and service providers will identify themselves to each other using Public Key Infrastructure identity

credentials, then service providers will check to see whether attributes about the consumer (a person or another computer) show that the consumer should be given access. As examples, these attributes might be associated with a person's role, with a person or a computer's organizational affiliation, or with geographic location. We have published standards for this new form of access control (called attribute-based access control or ABAC), and are partnering with the military services and with NSA to build and use prototype versions.

The Net-Enabled Command Capability (NECC) Program will enable decision superiority via advanced collaborative information sharing achieved through vertical and horizontal interoperability. NECC uses a tailored acquisition approach designed to rapidly deliver a series of smaller, tightly coupled command and control capabilities to implement capabilities as they become available. This new approach is envisioned for development, test, and certification. DISA is defining a highly interactive development and evaluation process called the Federated Development and Certification Environment (or FDCE) to enable agile provisioning of services on the network, and to ensure that service providers and service consumers understand each other's requirements. The Joint Combat Capability Developer (JCCD) for NECC is Joint Forces Command (JFCOM). They will define the "what". The Federated Development and Certification Environment will provide the means; and the Combined Test Force will ensure that capabilities and services can operate on the network and provide warfighting advantage. Per our Adopt before Buy, Buy before Create model, we will leverage existing and emerging capabilities as NECC components. Later this year, DISA will define and pilot a modified certification and accreditation process that will fit into the Federated Development and Certification Environment. As we work out the kinks, I expect this new certification and accreditation process to become the Department standard.

Mr. Chairman, I would be remiss if I did not mention other DISA missions providing critical support to the President and Defense Department. The first of these is the White House Communications Agency or WHCA that provides communications for the President, Vice President, and senior White House staff both on the 18 acre White House

compound and when they travel. We have modernized the capabilities used to support the President over the past five years and we have programmed to continue the modernization throughout the Fiscal Year Defense Plan.

We also provide critical support to the Defense Department through the Joint Interoperability Test Command or JITC and the Defense Spectrum Organization. The JITC provides interoperability testing and certifications for all joint communications and information technology systems acquired by the Department. The Defense Spectrum Organization provides support to the Secretary in ensuring the Department has the radio spectrum frequency agility needed to allow us to operate globally. It also provides technical support to deploying warfighting forces to de-conflict frequency congestion and solve interference problems.

Spectrum is extremely important as an enabler for net-centric operations and warfare. 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 DoD. 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 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. DISA is supporting two key initiatives to achieve transparent spectrum access for net-centric: 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.

I would now like to discuss our major transformational success as a Joint Acquisition Agency.

DISA has implemented a phased approach for enterprise information technology capabilities and services. The Agency acquisition workforce consists of highly trained and skilled professionals who understand the importance of surety, reach, and speed as components of the Agency strategy. We adopt innovative ideas and processes to deliver capabilities and services to close the gap between the availability of technologies and fielding them for warfighting advantage. In this regard, speed of delivery is often more important than a perfect solution.

We follow the precepts of "adopt-before-we buy" and "buy before we create" based on a best value assessment. If another organization has developed or acquired a capability or service that either fits or is close to fitting a need we have, we adopt it. Where opportunities are not available, we turn to the private sector and acquire a capability or service that either fits or is close to fitting the need. In both cases, we will perform a risk

analysis working closely with the operator 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. Our final choice is to create or build and we intend to avoid development and turn to others for solutions when we can. We will pursue the "adopt-before-we-buy" and "buy-before-we create" approach as a way of getting the 80-percent quality solution in the hands of the warfighter more quickly.

Consequently, we tailor our acquisition approaches and are developing innovative relationships with industry partners for strong performance-based solutions, speed, risk balance, and mission assurance. The following examples exemplify the use of tailored acquisition approaches.

Our Agency is implementing the DoD Teleport System. This system integrates, manages, and controls a variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence. The system is a telecommunications collection and distribution point, providing deployed warfighters with multi-band, multimedia, and worldwide reach-back capabilities to the DISN that far exceed current capabilities. This new system provides additional connectivity via multiple military and commercial SATCOM systems, and it provides a seamless interface into the DISN. The Teleport Program employed an evolutionary acquisition approach designed to maximize use of commercial off the shelf technology to provide capability to the warfighter as quickly as possible. The program is being incrementally fielded in generations, with each generation further broken down into capability increments. By maximizing existing technology, the program entered Generation 1 at Milestone C. We are working with the Services to take advantage of their expertise. For example, we are leveraging the Navy's UHF, EHF, and Teleport Management and Control Segment (TMCS) capabilities and the Army's Ka, IP, and Baseband capabilities.

Within the Commercial Satellite Communications program, we are proactively improving commercial SATCOM for the warfighter. The program office has cut provisioning timelines down from (as reported in a GAO report) a 79 day average to the current median of 21 days. Contracting and engineering fees have been reduced from 8% to 3.41%. Customer satisfaction ratings (using a 5 point scale) have increased from 3.9 in fiscal year 2005 to 4.5 in fiscal year 2006. In addition, business process reengineering is underway using the Lean Six Sigma model.

The Net-Centric Enterprise Services (NCES) Program is employing acquisition streamlining and speed of delivery concepts that include managed services provided by government and/or commercial industry. We execute accountability and service delivery using performance agreements such as Memorandum of Agreements, Service Level Agreements, and Performance Work Statements. We use broad Statements of Objectives supplemented with NCES specifications to communicate requirements. The service provider is responsible for life cycle management. Early user testing combined with developmental testing, demonstrations and operational assessments are used to identify gaps and provide information to support Limited Operational Availability (LOA) decisions. LOA decisions afford a declaration of user confidence to determine a capabilities ability to support a specified user base. LOA decisions also provide useful capability during the System Development and Demonstration Phase and assessment criteria based on service/capability type and associated risk.

As I mentioned earlier, the Net-Enabled Command Capability (NECC) program will use the enterprise services provided by NCES and will lead our efforts in streamlining acquisition of services and capabilities. I'd like to re-emphasize that NECC uses a tailored acquisition approach designed to rapidly deliver a series of smaller, tightly coupled command and control capabilities implement capabilities and services as they become available. This new approach will couple users, developers, testers, and certifiers in concurrent development, test, and certification. Again, we call this the Federated Development and Certification Environment, or FDCE.

As I said earlier, we will continue to develop innovative relationships with our industry partners. One example that we discussed earlier was the managed services concept employed by the Net-Centric Enterprise Services (NCES) program. We are also employing a capacity-on-demand services concept to acquire data processing and storage as services provided by vendor partners on our data center floors. We pay only for the capacity that is needed. This approach has the benefits of reduced time to add capacity, simplified cost drivers, streamlined operating system management, and facilitated technological currency. It is our intent to expand the concepts as appropriate to other capability requirements.

The Department of Defense has allowed DISA to tailor acquisition processes and use industry partnerships to accelerate providing capability to the warfighter. From an acquisition perspective, we believe our major challenge is clear. Specifically, we need to continue to accelerate speed of delivery, embrace risk-based testing, right-size the information assurance (IA) certification, support streamlining the requirements process, and support timely decision making as embraced by the Under Secretary of Defense for Acquisition Technology and Logistics in the Lean Six Sigma approach to streamline acquisition oversight. All these actions are required to reduce cycle time so that capability can be delivered to the warfighter inside the proverbial 18 month information technology change window. Capability must be deliverable before technology changes.

I'd like to turn now to Information Assurance.

Our efforts at DISA and at the JTF-GNO in information assurance are aimed at achieving two fundamental department-wide goals. First, DoD missions must continue to function well in spite of a cyber attack against the department's information infrastructure. Second, the department and its partners must be able to keep a secret when we need to, while at the same time being able to share information as broadly as possible. These are tough goals given the enormous complexity of the department's infrastructure, and can only be achieved by coordinated effort amongst all DoD entities responsible for acquiring

and operating portions of the information infrastructure. Clearly information assurance is a team sport, and we are teamed with the combatant commands, the Joint Staff, the Office of the Secretary of Defense, the military services, the National Security Agency, and many other department, federal, coalition, and industry partners in our efforts.

As JTF-GNO Commander, I am responsible for operating and defending the Global Information Grid (GIG). This responsibility flows from responsibilities given to the United States Strategic Command. Like any JTF commander, I have component forces from each of the military services.

DISA has several core roles in DoD information assurance. One is to ensure that the products we provide have appropriate security built into them. An example of this is the security being built into the Net-Enabled Command Capability program. A second role is as a provider of many of the core standards, processes, products, and services necessary to the establishment and maintenance of cyber defense-in-depth, and cyber attack detection and reaction capabilities across the department. In this DoD-wide role, DISA is teamed closely with the JTF-GNO. I would like to focus on that role here.

I will start by describing what we're doing to help DoD achieve the basics of information assurance, then I'll describe how our efforts are changing to anticipate and adapt to ongoing changes in DoD initiatives and to changes in information technology. Our programmatic efforts are done as part of the overall DoD Global Information Grid (GIG) information assurance portfolio, or the GIAP.

The basics start with secure configuration. This means ensuring that every device in the information infrastructure is configured as securely as possible. It also means that as vulnerabilities are discovered, device configurations are updated and devices patched as quickly as possible, and that the right people know the state of configuration of the infrastructure.

Secure configuration of devices starts with someone determining what a secure configuration actually is. DISA is partnered with the National Security Agency, with the National Institute of Standards and Technology, and with industry and non-profit entities in the production of guidebooks that describe the proper configuration of a particular operating system, for example. The DISA guides are called Security Technical Implementation Guides (STIGS) and are used throughout the department and elsewhere.

Discovery of a new vulnerability will often trigger changes to these standard configurations. The JTF-GNO tracks vulnerabilities, and when one is discovered that poses significant risk to the department, the JTF-GNO will issue an information assurance vulnerability alert, or an IAVA. An IAVA directs that certain remediation actions be taken by all in the department who administer systems, and directs that all units report compliance with the IAVA. On the unclassified and secret networks, DISA maintains web sites that contain the patches for operating systems and applications that system administrators require in order to comply with IAVAs. These sites ensure that DoD system administrators can get patches from a DoD entity, without having to compete with others on the Internet for access to vendor sites. DISA also acquires and operates a system used by DoD organizations to report compliance with IAVAs and other orders given by the JTF-GNO.

Proper configuration of a complex operating system is very difficult, as is manual verification of compliance with the configuration standard. To help system administrators determine the specifics of a device's configuration, and to help automate the process of changing configuration, DISA has acquired enterprise licenses for a configuration scanning/vulnerability scanning tool and for an automated remediation tool. We did these acquisitions under the oversight of the Computer Network Defense Enterprise Solutions Steering Group, an entity chartered jointly by the ASD (NII) and by USSTRATCOM, and co-chaired by the JTF-GNO. JTF-GNO mandated the use of these tools throughout the department, with the scanning tool as the first priority. The military services field and use the tools, with DISA providing fielding support.

Going forward, we are working with the National Institute of Standards and Technology and the National Security Agency to define industry standards for the description of vulnerability, of configuration, and of compliance measurement and we will then both produce our guidance documents to these standards, and we will purchase enterprise tools that comply with these standards.

In 2006 under the auspices of the Computer Network Defense Enterprise Solutions Steering Group, DISA let a DoD-wide contract for a tool that we call the Host-Based Security System, or HBSS. This is a piece of software that will sit on most computers in the department and will do a number of things associated with securing and reporting on these computers. Here are a few examples. The Host-Based Security System will further harden these computers against attack, including certain kinds of attack that have never been seen before but that are related to well-understood classes of vulnerability. It will also allow signatures that protect against emerging or rapidly spreading attacks to be pushed quickly to these machines. Going forward, it will also help to bring a machine back to a well understood configuration baseline, and thus remove malicious software that was not part of the baseline. The Host-Based Security System is being piloted at more than 20 sites throughout the department and will begin broad deployment later this spring.

Another part of the basics of information assurance is the provision of perimeter defenses for enclaves of computers. DISA builds and operates the primary perimeter defense between the DoD and the Internet as part of the overall Internet/DoD gateway system that DISA provides. This system is under the direct operational control of the JTF-GNO. The policy for what passes through this perimeter and what does not is set by the JTF-GNO and can be changed rapidly in response to changing threat conditions or other mission needs.

Most computers in the department are protected by several layers of perimeter defense, including the outermost one I just described. Some of these defenses are at the boundary between a military base and the department's core networks; some of these defenses are

located at the boundary between a tenant organization and a base; and still others are at the satellite communication gateways to deployed forces, or located in the deployed enclaves themselves. Policy at these shared perimeters defenses must be harmonized across the entire department to ensure that appropriate security is maintained while at the same time joint applications and business processes are not hampered by a local perimeter policy decision.

The JTF-GNO directs the perimeter policy at all large shared perimeter defenses in the department, supported directly by a DoD-wide risk management process run by DISA called "ports and protocols." The risks to computers inside an enclave of a particular network protocol are analyzed by DISA, and then a recommendation on whether the protocol should be allowed or denied is made to the DoD-wide risk management jury called the DISN Security Accreditation Working Group (or DSAWG). DISA chairs the DSAWG, with participation by the Combatant Commands, Services, Defense Agencies, and the intelligence community. The DSAWG's recommendations are forwarded to the JTF-GNO.

In order to shield most computers in DoD from direct attack from the Internet, in 2007 we will partner broadly to change the structure of perimeter defenses and of certain applications in the unclassified network. This effort will involve defining access zones in the network. Some of these zones will be visible to the outside world, some only to close partners, and some will have very restricted access. As part of the server consolidation going on in the military services, we will begin the movement of all publicly-visible and partner-visible servers into these more publicly visible zones. In cyber security jargon these more public zones are called demilitarized zones or DMZs. The servers in the DMZs will then act on behalf of the partner or on behalf of the public, and will reach back into the more restricted zones when necessary. This design is very similar to that used in large e-commerce companies to provide a rich customer experience while still protecting the back-end finance, inventory, and personnel databases. I expect that the application transition into DMZs will take several years. While we are moving to DMZs,

we are also modifying the design of the domain name system (or DNS) in the department, again to engineer what DoD looks like to the outside world.

A third part of basic information assurance is the use of strong, non-forgeable cyber identity credentials in information system access control, and in the signing and encrypting of documents and email.

Under the auspices of the NSA program manager, DISA acquires, operates, and sustains the DoD public key infrastructure (the DoD PKI). This infrastructure is used to issue two-part cyber identity credentials to all department uniformed, civilian, and on-site contractor personnel, and also provides a service somewhat analogous to a credit card checking service that allows an entity to check the revocation status of the credentials. The public part of the credential is distributed via a directory service that is part of the Public Key Infrastructure (PKI).

DISA and NSA have teamed with the Defense Manpower Data Center to issue the PKI credentials as part of the Common Access Card, or CAC, the standard DoD physical identification card. When someone gets a CAC, they also get both pieces of the PKI credential (the public half and the private half). The chip on the CAC protects the private half of the credential. DoD has issued more than 12 ½ million CACs, and since each CAC has multiple PKI credentials, more than 30 million PKI credentials have also been issued. The military services have deployed CAC readers and the associated middleware to most computers in the department.

As a means of reducing the department's vulnerability to password theft, last year JTF-GNO ordered that all logons to unclassified DoD computers be done via the PKI credential on a CAC. When a person logs in, the person inserts a CAC, then types a number to unlock the private half of the PKI credential on the CAC. The authentication service on the computer, or elsewhere on the network checks that the credential has not been revoked, then uses the public half of the credential to verify the private half. When these checks are satisfied, and if the person is an authorized user of the computer, access

is granted. No password is sent over the network, or stored anywhere other than on the CAC. This, combined with the fact that a physical CAC must be present to log in eliminates some methods of attack and makes others much harder. As of March 2007, 92% of logons to unclassified computers in the department were done using this method.

Additionally, all web servers on the unclassified and secret networks have PKI identity credentials. This year the JTF-GNO will require the use of a person's PKI credential to access "private" unclassified DoD web sites. Since both the person and the web site have PKI credentials, both can verify the authenticity of the other, all without passwords. This will improve security for the information contained in the web sites, and should also help ensure that the end-user is dealing with a genuine DoD web site.

In 2006, the JTF-GNO also directed an increase in the Information Condition, or INFOCON, of the department. As part of this, the JTF-GNO directed implementation of a package of initiatives intended to reduce vulnerability to certain types of attack even further. The most visible of these initiatives was the direction to stop allowing DoD personnel to use a web interface to access their DoD-email. This direction was a result of the fact that most web-based mail systems can only use a user name and password for access, not the stronger CAC/PKI combination. Like all JTF-GNO orders, the web-mail order was first issued as a warning order, and comment on the mission effect from the order was invited from all in the department. The JTF-GNO considered this input, and then issued the final order. Like most broad JTF-GNO orders, this order contained a safety net; exceptions to the policy could be made by people at the three star level or higher. Few of these exceptions have been granted, and DoD has become much more resistant to password-guessing attacks directed at web mail.

We measure compliance with all these initiatives in several ways. First, the JTF-GNO gets reporting on compliance from their components, and from the other organizations of the department. Second, DISA sends teams, under the direction and sponsorship of the JTF-GNO, to selected sites throughout the department. These teams are called Enhanced Validation Visit teams, and report their findings both to the site visited and the JTF-GNO.

The findings are used to correct deficiencies at particular sites, and are also used by various DoD entities to understand systemic programmatic or operational problems.

In spite of all the emphasis on the basics, we know that our defenses will not be perfect, and that vulnerabilities will be found and exploited. As a consequence, DoD also requires the ability to spot attacks, then determine enough about the attack that militarily useful courses of action can be developed, selected, and executed. DISA and NSA acquire and operate attack detection and diagnosis systems at the gateways between the Internet and the DoD. Many attacks that traverse these gateways can be spotted and understood using these systems. The JTF-GNO is the primary customer of the output of these systems, although the information is used by network operations, or NetOps, personnel throughout the department.

DISA and the military services also operate attack detection and diagnosis systems within the department's networks. The DISA Theater NetOps Centers (TNCs) use the DISA-managed detection and diagnosis systems, along with reporting from the NetOps centers of the military services and the NSA, to provide a consolidated incident detection and reporting service to the various combatant commanders. These DISA TNCs are under the operational control of the JTF-GNO, and like the JTF-GNO, the TNCs combine network management and computer network defense personnel to provide the fastest problem diagnosis and resolution possible. These combined centers can more quickly do the triage associated with the question, "Is this a cable cut or a cyber attack?" for instance. The NetOps centers of the military services, as well as the TNCs, all report to the JTF-GNO, which consolidates the global view of incidents and coordinates responses across organization boundaries as required.

Like much other information technology in the department, the attack detection and diagnosis systems used by the military services and DISA were developed and deployed separately, since each organization had a different span of control. Under the auspices of the Computer Network Defense Enterprise Solutions Steering Group, DISA produced a consolidated DoD-wide plan for an enterprise sensor grid last year, and is currently

coordinating a broader attack detection and diagnosis plan which we expect to issue later this year. Additionally, we are pursuing an enterprise acquisition for insider threat observation and detection tools this year. The increased use of public key identity credentials, combined with such tools will allow us to construct a more capable insider threat detection and deterrence capability.

To ensure that the DoD standards for certain NetOps functions are well understood and followed, the JTF-GNO sponsors the Computer Network Defense Service Provider accreditation process (the CNDSP). Teams from DISA and from NSA evaluate operational entities throughout the department to a set standard, and then USSTRATCOM accredits organizations that meet the standard.

How are we doing? First, we are seeing improvements in the configuration of DoD computers. As a result of our configuration automation efforts, and as a result of increased management focus throughout the department, IAVA compliance climbed 136% from June 2006 to January 2007.

We are also seeing more reporting of cyber incidents in the department. In 2004, we had roughly 16,000 incidents reported. In 2005, this rose to roughly 23,000 incidents. In 2006, this increase continued, with a total of 30,000 incidents reported. A cyber incident is an assessed occurrence having actual or potentially adverse effects on an information system. The incident numbers I gave do not include the high amount of scanning data -- roughly 4 times the numbers I just stated. I attribute these increases in reporting to our emphasis on better reporting, and on better operational procedures and technology for detecting attacks. I'd like to emphasize that a major portion the majority of these incidents are *unsuccessful* attacks.

The number of successful attacks declined from roughly 130 in the month of January 2005 to roughly 40 in January 2007. I attribute this decrease to improved configuration control of computers, including that of web servers; the elimination of many passwords, and our focus on perimeter security. A subset of the successful attacks is the number of

DoD computers used in botnets. A botnet is a large network of compromised computers that is typically rented to the highest bidder. Botnets are typically built using completely automated attacks. While botnet activity in the Internet increased roughly 110% from February 2005 to December 2006, during the same period, the number of DoD computers used in botnets *decreased* by 61%.

One more trend I'd like to mention. Our hardening efforts are changing the behavior of certain adversaries. As configuration, password, and some network vulnerabilities are going away, attackers are moving "up the stack" and focusing on data-driven attacks. An example of this is the increase in bogus electronic mail attacks, sometimes apparently coming from a legitimate source. We went from three email attacks reported in January 2006, to a high of 161 email attacks reported in September 2006. This declined to 61 reported attacks in December 2006 as we directed that everyone in DoD be trained to recognize and counter these attacks, and as access to web-mail declined.

Thank you, Mr. Chairman and members of the subcommittee for inviting me to testify before you today. That concludes my formal testimony and I would be happy to answer any questions to the best of my ability.