RECORD VERSION

STATEMENT BY

MR. ROBERT F. LENTZ

DEPUTY ASSISTANT SECRETARY OF DEFENSE,

FOR CYBER, IDENTITY AND INFORMATION ASSURANCE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

SUBCOMMITTEE ON

MANAGEMENT, ORGANIZATION AND PROCUREMENT

May 5, 2009

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Good afternoon, Chairwoman Watson, Congressman Bilbray, and Members of the Management, Organization and Procurement Subcommittee. I am Robert Lentz, the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance representing the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. I am also the Department's Senior Information Assurance Officer. I am pleased to appear before the Subcommittee to discuss initiatives to enhance the Department's and the nation's information assurance/ cybersecurity posture.

Information assurance/cybersecurity (IA/CS) is a critical priority for the Department of Defense (DoD). With information and information technology (IT) assets distributed over a vast and wide-ranging enterprise and with diverse domestic and international partners actively participating in DoD missions, we know that we cannot execute operations without the Global Information Grid (GIG) – our DoD network. The GIG is not just a collection of individual networks that happen to share the same Internet access points; the GIG is how we operate; the GIG is where business goods and services are coordinated; where medical information resides; where intelligence data is fused; where weapons platforms are designed, built and maintained; where commanders plan operations and command and control forces; and where training, readiness, and morale and welfare are sustained.

Therefore, the Department is focused on building and operating the GIG as a joint global enterprise that can be depended on wherever we operate in the world and under any circumstances to include cyber attack. This enterprise network approach, coupled with skilled users, defenders, and first-responders and in partnership with the intelligence community, will allow us to more readily identify and respond to cyber attack – and still accomplish the mission.

The DoD cyber, identity and information assurance (CIIA) program is thus aimed at ensuring the following vision:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform as expected.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The Defense information environment securely and seamlessly extends to mission partners.

Strategic Goals

To realize this vision, the Department has established four strategic IA/CS goals:

Goal 1: Organize for unity of purpose and speed of action. This goal focuses on how IA/CS is considered as the Department plans for and evaluates use of cyber assets or the cyber domain in Defense missions, the development and sustainment of our IA/CS workforce, and the expansion of IA/CS capabilities and capacity through partnerships, whether they be intra-government, with academia, with information technology (IT) industries, with defense industries, or with our international and military coalition partners.

Goal 2: Enable mission-driven access to information and services. This goal addresses how the Department securely delivers the power of information to its warfighting, intelligence, and business communities.

Goal 3: Anticipate and prevent successful attacks on data and networks. This goal addresses how the Department configures and instruments the GIG with tools and technologies to prevent intrusions, detect intrusion attempts, and reduce attack surfaces to deny adversaries any opportunity or advantage.

Goal 4: Prepare for and operate through cyber degradation or attack. This goal addresses how the Department creates trust and confidence in its weapons systems, data, and networks; strengthens its IA/CS readiness; operates in a degraded cyber environment; and restores cyber capabilities.

These goals provide the means to protect and defend the GIG today and to improve IA/CS capabilities over time. We are progressing toward an enterprise information environment that can dynamically and automatically configure itself to counter any threat and facilitate any mission.

The Department has made significant advances toward the vision. We have:

- Joined forces with other federal agencies in a comprehensive national cybersecurity[1] initiative to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed a DoD Information Management/Information Technology (IM/IT) Strategic Plan to further transition to net-centric operations to achieve information advantage.
- Recognized cyberspace as a global domain within the information environment, developed a National Military Strategy for Cyberspace Operations (NMS-CO), embraced a Network Operations (NetOps) construct for operating and defending the GIG, and, under United States Strategic Command (USSTRATCOM), integrated NetOps with other cyber operations.
- Stood-up and connected key cyber centers such as the National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), and the Defense Cyber Crime Center (DC3) as well as certified all 25 network defense centers across DoD.
- Operationalized the Joint Task Force for Global Network Operations (JTF-GNO) under USSTRATCOM.
- With industry and academia, developed the IA Component of the GIG Integrated Architecture and plans and programs for delivering key identity and IA/CS capabilities as enterprise services.

[1] The U.S. Government currently defines *cybersecurity* as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (NSPD 54/HSPD 23).

- Partnered with the Director for National Intelligence (DNI) to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of all levels of classified/sensitive information and to protect sensitive or controlled unclassified information to include sharing with our closest partners.
- Established a cybersecurity program in partnership with the Defense Industrial Base (DIB) to protect unclassified information relevant to Defense-related research, development and procurement.
- Established DoD policy addressing the relationship between cyber offensive and defensive actions called Computer Network Defense Response Action (CND RA).
- Worked with the National Counterintelligence Executive (NCIX) and Insider Threat Advisory Group to foster collaboration on the use of insider threat IA/CS tools.
- Created a DoD Venture Catalyst Initiative called DeVenCI to aid in the invention of cutting edge IA/CS solutions.
- Developed a comprehensive IA/CS policy framework that ranges from identity protection to wireless and satellite security to workforce training and education.
- Created the National Cyber Response Coordination Group in partnership with the Departments of Homeland Security and Justice.
- Launched a comprehensive cryptographic modernization initiative.
- Established a trusted foundry program and sought ways to improve microelectronics and software assurance.

The breadth and depth of all the programs and initiatives underway within the Department is too large to cover here. However, I would like to highlight a few current enterprise initiatives within the DoD CIIA program, organized by our strategic goals.

Goal 1

In support of Goal 1 (Organize for unity of purpose and speed of action), I will highlight our efforts to establish a DoD cyber workforce, partner with the DIB in a cybersecurity pilot, and build an international IA program.

Workforce

While our long-term aim is to achieve robust machine-to-machine network defense capabilities, people will always remain our frontline against cyber adversaries. From the everyday user to cyber defenders, the DoD workforce needs to be fully trained and qualified in key areas, and appropriately deployed to leverage and protect the Department's tremendous investment in information and communications. Achieving a technically adept cyber-capable workforce is job one! Competency in multiple IA/CS skills along with extraordinary cyber expertise or "black belts" in specialty areas, plus joint exercises to foster greater knowledge throughout the cybersecurity community has become a core priority of the Department.

To this end, the Department is continuing to expand the range and quality of IA/CS training available to its workforce. The technical schools of the military services have expanded their IA/CS curricula to meet DoD common baseline training and certification requirements. For example, the Air Force’s school at Maxwell, AL, and the Navy’s program at Pensacola, FL, are offering tremendous new programs. The Defense Information Systems Agency (DISA) sponsored Carnegie Mellon Virtual Training Environment provides real-time, on-line interactive IA/CS technical training to both military and civilian workforce members wherever they are in the world. The Information Resource Management College (IRMC) at the National Defense University here in Washington, DC now offers an advanced IA/CS curriculum supporting baseline standards to both DoD and federal leaders in all Departments. The military service academies and post-graduate schools are also heightening focus on IA/CS. Recently, the Army, Navy, and Air Force academies competed in the ninth-annual cyber game for cyber warriors.

The Department has a rich suite of simulation and exercise tools analogous to flight simulators that create realistic and secure environments for training and practicing IA/CS skills. This approach provides opportunities to “see” and respond to threats in a controlled environment, and rapidly build skills and experience without disrupting operational networks.

The Department has also developed IA/CS awareness training to help users and leaders to better understand their roles in defending DoD networks. The 2009 DoD IA Awareness training product introduced a new more interactive approach to teaching end users about their critical role in securing our networks. Our compliance reports show that 2.1 million personnel successfully completed this user awareness training program. Leadership development curricula in the military service and Joint Professional Education Programs have increased emphasis on IA/CS awareness to improve operational leaders' understanding and support for CIIA requirements. Operational leadership support is critical for effective execution of IA/CS activities at all levels.

The National Centers of Academic Excellence in IA Education (CAE) are producing graduates with the right skills to achieve a world class cyber workforce that includes both defensive and offensive capabilities. The CAE and CAE-Research (CAE–R) programs reduce the vulnerability of our nation's information infrastructure by promoting IA higher education and research and by producing a growing number of professionals with IA expertise in various disciplines. Currently, there are 94 CAEs across 38 states and the District of Columbia, including five military academic institutions: the Air Force Institute of Technology, the IRMC, the US Military Academy at West Point, the Naval Post-Graduate School, and the US Air Force Academy. For many students, especially graduate students, research is their "true educational experience." We must continue to expose these students to our hardest problems. The aim of the CAE-R program is to advance IA technology, policy, and operations that enable the nation to effectively prevent or respond to catastrophic cyber events. The CAE-R designations total 23 IA research centers across 17 states and the District of Columbia.

The CAEs provide DoD with many partnering opportunities. One example is the *Wounded Warrior Training Program* for America's wounded, disabled, and transitioning veterans. Mississippi State University's Forensics Training Center, in collaboration with Auburn and Tuskegee Universities in Alabama, is providing no-cost vocational training to veterans in a critical technical shortage area – digital forensics. In the fall of 2008, the Department helped bring this training program to the Walter Reed Army Medical Center in Silver Spring, MD. The intent is to offer the program for recovering military personnel at other major hospitals across the country this year and beyond.

Currently the Department is evaluating partnerships with University of California, Davis and University of North Carolina, Charlotte for *secure software development education*, including secure coding clinics for students. The intent is for students to receive an in-depth introduction to secure software techniques, have access to the tools and methods used to fix software vulnerabilities, and understand how to use them. The partnership, if undertaken, would be a key step in providing critical and leading edge software engineering skills to students who are potential DoD or federal employees.

Defense Industrial Base

In early 2008, the Department initiated a DIB Cyber Security and Information Assurance (CS/IA) pilot program to address cybersecurity risks to DIB unclassified networks that support DoD programs. The DIB CS/IA pilot has five major components: a binding bilateral DoD-DIB company framework agreement to facilitate CS/IA cooperation; threat and vulnerability information sharing; DIB network incident reporting; damage assessments; and DoD acquisition and contracting changes, including proposed changes to Defense Federal Acquisition Regulation Supplement (DFARS). The DoD-DIB legal framework provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected.

Under this program, the Defense Cyber Crime Center (DC3) is the focal point for threat information sharing. DC3, in coordination with other cyber centers, analyzes and disseminates near real-time threat information. To further strengthen near real-time information sharing and collaboration between DoD and its DIB partners, DoD is developing a secure electronic data/voice communication network called DIBNet. The DC3 also performs digital forensic analysis on reported DIB intrusion sets. These processes are labor intensive and require resources and advanced skills.

The Damage Assessment Management Office in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics orchestrates our military service damage assessment cells and is helping to standardize methodologies. Through damage assessments, the Department will be able to better determine the extent of compromised DoD information, as well as assess the overall impact of the compromise on current and future weapons programs, scientific and research projects, and warfighting capabilities.

The DIB CS/IA pilot is informing proposed changes to the DFARS for enhanced IA/CS requirements in DoD contracts.

To continue improvements in DIB network security, the Department of Homeland Security, in collaboration with the Department of Defense, is evaluating the DIB model for sharing cybersecurity information with other Critical Infrastructure sectors.

International Program

The Department has a very robust program built on trusted bilateral, multilateral, and institutional relationships with national and military representatives around the world to enhance situational awareness and capabilities to counter common cyber threats, share tactics, techniques and procedures and synchronize IA/CS strategies and policies. Shared situational awareness helps stay ahead of the threat, protects U.S. secrets and sensitive information residing on foreign networks, and protects coalition and allied operations, especially with increased ops tempo for counterterrorism activity and for peacekeeping. Cyber attacks in Estonia and Georgia have accelerated international cooperation. A common objective is to promote adoption of international standards and norms in partnership with interagency processes. This includes developing common positions for international fora, influencing standards and technology, and discussing international norms of behavior in cyberspace.

We have a number of bilateral agreements with partner countries and are aggressively pursuing more. Current activities include the International Computer Network Defense

(CND) Coordination Working Group (ICCWG), the International Cyber Defense Workshop (next one is June 2009), international civil and military participation in Cyber Storm II, (a large-scale national cyber exercise part of Homeland Security's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector), and the ongoing sharing of best practices, policies, and threat information. Challenges in this area include limited classified network connectivity, over-classification of information, and difficulties in applying "write for release" practices for cybersecurity information sharing.

Goal 2

Next I will highlight two initiatives under Goal 2 (Enable mission driven access to information and services). They are identity management and assured information sharing.

Identity Management

Our identity management (IdM) initiative provides the ability to identify people and devices on our networks and distinguish among friendly, neutral, and unfriendly entities. Our Identity management capabilities are based on use of public key infrastructure (PKI) technology. Our public key certificates and the Common Access Card (CAC) provide strong, highly trusted electronic identity credentials for our people and our non-person entities (e.g., network and computer devices, phones, radios, satellites, services, applications, etc.). The Department’s PKI and IdM efforts are base-lined on the Homeland Security Presidential Directive 12/Personal Identity Verification (HSPD-12/PIV) standard for the Federal Identity Credential. Nearly all of the Department’s Active and Reserve military, civilian employees and contractors utilize CACs to facilitate network, web site, and facility access. Adherence to the HSPD-12/PIV identity credential standard makes it possible for federal partners to use their PIV cards to access DoD information repositories and web servers with enhanced user security.

The Department’s use of hardware-based identity credentials for access to networks and information systems has shut down known attack vectors, demonstrably decreased attacks, and elevated the security posture to our networks by denying anonymity to attackers. The use of biometrics in conjunction with PKI credentials is yielding important improvements in protection against insider threats. Identity interoperability with industry and international groups will help with secure information sharing and force protection.

DoD is involved in two premier programs leveraging standardized identity credentialing. They are the Transglobal Secure Collaboration Program (TSCP) and the Federation for Identity and Cross-Credentialing Systems. The DoD and industry have partnered through the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) to verify the identity of personnel and accept each other's identity credentials. FiXs currently verifies and authenticates the identities of contractor personnel seeking to enter U.S. military installations or other government controlled areas.

The Transglobal Secure Collaboration Program (TSCP) is a government-industry partnership specifically focused on facilitating solutions to the most critical issues in Aerospace and Defense (A&D) today: A key enabler for the TSCP is a common identity approach that is highly aligned with the HSPD-12/PIV credentialing program. Their interoperable identity credentials mitigate the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions. To do business in the world today, A&D companies must balance the need to protect intellectual property (IP) while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information. This duality requires that security be both within organizations and across extended supply chains and partners.

Assured Information Sharing

In addition to sharing information among trusted users across organizational boundaries, the Department is working hard to enable sharing across the entire spectrum of security domains while protecting networks and information. To that end, it partnered with the DNI and established the Unified Cross Domain Management Office (UCDMO) in 2006. The UCDMO is staffed with personnel from throughout the Department of Defense and the Intelligence Community (IC); it provides centralized coordination and oversight of all cross domain activities and ensures a common approach for the implementation of cross domain capabilities within the Department and the IC. Additionally, it is working to ensure that secure, robust and flexible capabilities are available and extensible to share information among federal, state, local and tribal entities and with mission partners and private sector enclaves appropriately. The UCDMO roadmap is aligned to the information sharing strategic plans of the Department and the IC, and it is focused on delivering needed sharing capabilities, providing return on investment, managing security risk, and promoting awareness and collaboration among the users and developers.

Goal 3

From Goal 3 (Anticipate and prevent successful attacks on data and networks) I will highlight two initiatives; network de-militarized zones and host-based security. This goal is focused on hardening data and networks in order to anticipate and prevent successful attacks on them. The most capable and motivated of our adversaries will use any means available to achieve their goals, and our strategy must address that range of tactics. To that end, we invest in intelligence and perimeter-hardening to anticipate and prevent successful attacks, but we also design and configure systems to ensure that attackers are easy to find and/or contain should they pierce perimeter defenses.

De-militarized zones

Network de-militarized zones (DMZs), are to perimeter defense as a moat is to a castle. The DMZs obviate the need for most DoD assets to ever have to touch the Internet. Instead, those DoD applications, such as email, which must face the Internet are housed within a special containment zone. Within that zone inward-bound traffic can be carefully scrutinized for viruses and other malware. The DMZ controls can also enforce white-listing, that is, only allowing traffic from trusted addresses to enter the enterprise, and perhaps most importantly, by acting as a proxy for all communication to the untrusted world, can deny adversaries reconnaissance knowledge of the structure of DoD networks. The Department has vastly reduced the number of its Internet access points, the first step in moving toward an enterprise-wide DMZ architecture, and is identifying outward-facing applications for placement in the zones.

While DMZs harden the network at entry points, host-based security provides a line of defense at each computer. Host-based security significantly reduces the risk of cyber attack at the individual computer by preventing malicious code and unauthorized applications from running. It also provides a consistent way to do configuration and management across all DoD networks.

Host-based security

Host-based security includes, but is not limited to host firewall, host intrusion detection, host intrusion prevention, system compliance profiling, rogue system detection, application blocking, and Information Condition (INFOCON) baselining. Under USSTRATCOM's direction, the Department is rapidly implementing host-based security across the enterprise. It is now deployed within approximately 40% of the host processing environment, and should be deployed to a majority of our systems by early 2010. Coupled with this, we are widely deploying the Federal Desktop Core

Configuration, a pivotal industry/government cooperative venture, beginning with ubiquitous Microsoft products, to make computers more stable and defensible. We are also widely deploying data-at-rest protection.

As is evident from these highlighted projects, safeguarding our networks against adversary attack today requires close partnership between information assurance experts and information technology (IT) providers. The DMZs are as much about network architecture as they are about specific tools for content filtering, and host-based security is a suite of software which is installed on commodity computing hardware; it is not a stand-alone IA device that plugs in to a computer or network. This convergence of IA/CS and IT poses challenges for governance and training, but it promises some new and much more efficient ways to secure our networks.

Our DoD research labs are particularly interested in new IT paradigms that change the game for defense, and I will close this section by discussing two of them, virtualization and cloud computing, which together and separately may revolutionize how we think about and secure our networks.

Virtualization

The DoD enclaves today look mostly like traditional local area networks; each user has a physical device on a desk linked back to one or more servers. Some user data lives on the desktop machine and some resides on servers, with the desktop patched periodically to close security holes and implement new configuration guidance. With virtualization, the necessity for coupling together specific logical and physical assets goes away. For example, each user's environment (data and computing tools) can be stored and maintained as a digital file or image in a central control area. When a user needs their environment, it can be "incarnated" into any compatible physical platform. So tomorrow, instead of scanning physical components for current state and applying patches to bring the component into compliance, we may, instead, proactively repair and refresh the stored images and only incarnate the good ones. Doing this cleverly and often will make it harder for adversaries to sustain the footholds they gain through phishing attacks to persist in our networks.

Cloud computing

Cloud computing builds on these ideas to offer a virtual computing fabric with almost limitless and infinitely definable processing and storage capacity. In the future, many enterprises will choose not to invest in their own IT departments, but will pay as they go, relying on ability to access commercial computing services in the cloud. For many DoD applications, the commercial cloud will be too risky, but a private cloud could bring us many benefits. Besides the obvious economic benefits of scalable, on-demand computing, a private cloud also gives us the ideal platform with which to provide the virtual monitoring and provisioning described earlier. A cloud is also an ideal place from which to make capabilities available to the whole enterprise. While, in the DoD, we have encountered challenges moving towards a service-oriented architecture (SOA), in the private sector, companies like Google and Salesforce are basing their business models on an insatiable public hunger for software and applications as a service. Emulating their delivery mechanisms within our own private cloud may be key to how we realize the true potential of net-centricity.

Goal 4

Finally, I will highlight three initiatives under Goal 4 (Preparing for and operating through cyber attack or degradation) which provides a foundation to leap beyond traditional IA/CS approaches. They are supply chain risk management, assurance in defense system acquisitions, and network resiliency.

Supply Chain Risk Management

While the global marketplace provides the Department increased opportunity for innovation in information and communication technologies (ICT), it also provides increased opportunity for malicious actors to manipulate ICT products and services to gain unauthorized access to otherwise closed-off technologies and services – what we call supply chain risk.

Threats to the ICT supply chain can affect both software and hardware products. Software design, development, testing, distribution, and maintenance frequently can be done less expensively offshore, but puts technology within easy reach of malicious actors. At the same time, the growing complexity of software and microelectronics makes discovering vulnerabilities extremely difficult. Security of the ICT supply chain can also be compromised by untrustworthy or counterfeit ICT components. We are particularly concerned about the semiconductor industry which has increasingly moved toward offshore or foreign-owned semiconductor component production. This trend creates an increasing threat to the US as the potential for unauthorized design inclusions to appear on integrated circuits used in military applications increases.

As early as 2003, the Department promulgated a Defense Trusted Integrated Circuits Strategy. The Trusted Foundry Program, initiated in fiscal year 2004, leverages a contract with IBM to aggregate purchases of leading edge semiconductors with state-of-the-art features for use in defense applications. As part of the contract, IBM upgraded their facilities and implemented enhanced security procedures, creating the Department's first Accredited Trusted Integrated Circuits Supplier. In 2004, the Department tasked the NSA to stand up a new office to manage this contract and expand the ranks of suppliers capable of providing trusted integrated circuits. In response, NSA created the Trusted Access Program Office and implemented a trusted integrated circuits supplier accreditation program, now overseen by the Defense Microelectronics Agency.

The Trusted Foundry Program is funded at approximately $80M/year through equal investments from the Services and NSA as well as from direct program payments for chip processing and services. In 2008, the Trusted Foundry served over 80 program customers and processed 412 unique integrated circuits designs. The Trusted Supplier

Accreditation program continues to expand and there are now 21 Accredited Trusted Suppliers providing a full range of services enabling the department to draw on a fully accredited end-to-end trusted supply chain for integrated circuits.

Building on the Trusted Integrated Circuits Strategy, the Department continued to work supply chain risk issues both internally through DoD software and systems assurance efforts beginning in 2004, and within the interagency through the Committee on National Security Systems. Its strategy is holistic: System prioritization allows the Department to apply resources first against our most critical systems; an approach to driving assurance activities into the systems engineering process, to identify critical sub-systems and components, and to mitigate vulnerability through engineering design; a supplier assurance process to increase knowledge of counterintelligence threats posed by the suppliers' chain; a technology strategy to improve vulnerability detection capability, and a collaborative effort between DoD and industry to identify standards and best practices. This approach was validated by a September 2007 Defense Science Board study "Mission Impact of Foreign Influence on DoD Software," and informed subsequent efforts within DoD and the interagency.

The Department now co-leads an interagency effort with the Department of Homeland Security to develop a multi-pronged, US Government (USG)-wide approach to global supply chain risk management for hardware and software ICT. This effort brings to bear a range of USG capabilities to address national security risk to USG systems and networks from globally developed and maintained ICT through sharing of technical risk mitigation techniques, development of new acquisition guidance, work with industry on the promulgation of commercial standards, and enhancement of IT and software assurance capabilities. The Department has recently issued policy for managing supply chain risk to ICT within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23. Additionally, the policy establishes Department-wide responsibilities for meeting the assessment and reporting requirements of §254 of the Fiscal Year 2009 National Defense Authorization Act.

The Department is incrementally developing a supply chain risk management (SCRM) capability, beginning with pilot activities in fiscal years 2009-2010 and progressing to full operational capability by fiscal year 2016. These pilots are a joint effort led by the Deputy Assistant Secretary of Defense for CIIA. Each of the military services and DISA has identified pilot programs to test SCRM engineering and procurement processes and mitigations and share best practices. The Department is also partnering with the IC in evaluating the risk to the Department posed by commercial entities conducting business with the individual components of the Department.

Ultimately the goal of the SCRM pilots is to position supply chain risk management decision-making very early in the system lifecycle. Early identification of risk facilitates mitigation through system design and ensures that ICT products purchased for use on DoD systems and networks are sufficiently trustworthy for their intended purpose.

Assurance in Defense System Acquisitions

Complementary to the SCRM efforts are the DoD CIO's responsibilities for overseeing the integration of IA/CS into major defense system acquisition programs to ensure compliance with statute, and consistency with DoD policies, standards and architectures. Under Subtitle III of Title 40, United States Code (formerly the Clinger-Cohen Act of 1996), the Department conducts formal reviews of the acquisition IA strategies of all Major Automated Information Systems (MAIS) and Major Defense Acquisition Programs (MDAP) prior to approval of all acquisition milestone decisions. The acquisition IA strategy sets the stage for early, effective, and efficient implementation of IA into the system.

The Department emphasizes the early identification of IA/CS requirements for all IT acquisitions, including weapons systems and command and control systems. An IA/CS controls-based approach is employed that mandates a comprehensive set of protection requirements based on the sensitivity of the information and the importance of the mission that the system supports. The specific IA/CS technical solutions that satisfy the individual IA/CS controls must be certified as effective and secure before implementation into the systems. Leading-edge networking programs are required to comply with similarly leading-edge information security requirements from NSA to ensure that new capabilities are protected. Finally, the system as a whole is subjected to a rigorous independent security review and an overall risk management decision prior to allowing it to operate. The Department is working to streamline the fielding of ICT commercial solutions, accelerate the certification and accreditation process, and achieve greater reciprocity of IA/CS risk management processes and decisions across the Department and federal government.

A particular challenge in this area is acquisition time. Our reliance on globally sourced ICT means our adversaries have access to the same technologies we do; however, our ICT and IA/CS acquisitions must follow the same rules as for weapons systems, constraining our ability to respond quickly. We need more agile ICT and IA/CS acquisition processes. Acquiring automated information systems without a production component is significantly different from acquiring a weapons system. For weapons systems we concentrate on key risk areas like technology maturity and producing large numbers of custom hardware in economic quantities. In contrast, for automated information systems we concentrate on reducing risk in areas like process reengineering, enterprise architectures, information assurance, and integration of multiple commercial off-the-shelf applications.

The challenges of information technology acquisition were studied by the Defense Science Board as directed in the fiscal year 2008 National Defense Authorization Act. The results of their study were recently released (April

2009) and recommended changes to our acquisition processes, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. A process that is agile and geared to delivering meaningful increments of capability in approximately 18 months or less.

DoD has recently instituted a new rapid intergovernmental acquisition process that develops multiple competitively-awarded Blanket Purchase Agreements (BPAs). In partnership with the General Services Administration (GSA), this process provides BPAs in six months for heavily discounted IA/CND products available for federal, state, local, and tribal government agencies.

Network Resiliency

Denial of service against critical elements of the physical and application layer of the networks and cyber attacks effecting the integrity and confidence of information flowing to users and decision makers is increasingly a major source of risk, as shown by recent undersea communications cable cuts or threats by software worms like Conficker. The Department's Guidance of the Development of the Force (GDF) for 2010-2015, signed May 2008 states, "All DoD Components will reduce the risk of degraded or failed missions by developing doctrine/tactics, techniques and procedures and planning for, implementing, and regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid."

In support, we have a series of cyber resiliency and mission assurance initiatives that are focused on reducing risks to missions should our networks, enterprise services, or information be compromised or degraded. They include:

- Exercising military operations under a severely degraded cyber environment.
- Improving prioritization for recovery and continuity of operations planning.
- Strengthening network command and control capabilities.

While the Department is aggressively enhancing the security of the GIG and promoting IA/CS nationally and internationally, the threats in an information-centric world are dramatic. Conducting counterterrorism operations, global peacekeeping, homeland security and preparing for escalated warfare make it imperative that IA/CS be viewed not as an IT expense but as a critical enabler of all national security and defense capabilities. To this end, the Department sees its participation in the Comprehensive National Cyber Initiative (CNCI) as imperative. The Department leads or co-leads several CNCI initiatives:

- Initiative 3, with the NSA supporting Department of Homeland Security efforts to secure the .gov domain.
- Initiative 7, with the Department and the DNI co-leading an effort to secure the classified networks.
- Initiative 8, with the Departments of Defense and Homeland Security developing the conceptual foundation for building the USG cyber workforce of the future and reinforcing the skills of the current workforce.
- Initiative 11, previously discussed under SCRM.

Summary

In conclusion, the Department has a strong IA/CS vision, strategy and supporting program. We are working toward a resilient and defendable core network for the Department and for the nation. The ASD(NII)/DoD CIO is managing a diverse portfolio to lead the Department toward Net Centric operations and aggressively working to get ahead of the daunting security challenges facing the Department.