

**Statement by
Robert F. Lentz
Director of Information Assurance
Office of the Assistant Secretary of Defense for
Networks and Information Integration
and
DoD Chief Information Officer**

**Before The
House Armed Services Committee
Subcommittee on
Terrorism, Unconventional Threats and Capabilities
Hearing on
Cyber-Terrorism**

July 24, 2003

Thank you Mr. Chairman and members of the Subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee about actions the Department of Defense is taking to address threats to the security of its networks, systems and information. We have and continue to make significant progress in our quest to secure and defend our computer networks. My testimony will highlight some efforts we have initiated, successes we have achieved and the challenges we face.

Secretary Rumsfeld, in one of his initial testimonies before the House Appropriations Defense Subcommittee, identified six key transformational goals for the Department around which we focus our defense strategy and develop our force. Leveraging information technology to create a seamless, interoperable, network-centric environment is one of those foundation transformational goals. As demonstrated in recent operations, U.S. Forces have unparalleled battlefield awareness; they can “see” the entire battlefield while the enemy cannot. They have translated information technology into combat power beginning the transformation from Platform-Centric to Network-Centric Operations. And the transformation has just begun. A new era of warfare has emerged, one based on the concept that connections provide greater power, agility, and speed. Multiple connections enable U.S. Forces to fight and mass combat effects virtually anywhere, anytime, and with a smaller "real" force. Through connections, smaller forces operating locally can leverage almost the full weight of global U.S. combat power. However, as our dependence on information networks increases, it creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting U.S. Forces. In recognition of this dichotomy, the Secretary established the protection of U.S. information networks from attack as another foundation transformational goal.

Emphasizing that transformation is not an event, Secretary Rumsfeld described it as an ongoing process, a journey that begins with a transformed “leading edge” force, which, in turn, leads the U.S. Armed Forces into the future. Mr. John Stenbit, Assistant Secretary of Defense for Networks and Information Integration and the DoD Chief Information Officer (CIO), is committed to support our transformation by providing the power of information to that leading edge. To bring power to the edge, he established the

following goals for his supporting effort: (1) develop a ubiquitous network environment, (2) richly populate with information of value, as determined by the consumer, (3) ensure the network is highly available, secure and reliable. My role in bringing power to the edge is to support Mr. Stenbit's goals by guiding and overseeing the Department's Information Assurance (IA) Program; the strategy, policy and resources required to create a trusted, reliable network.

No one agency, organization, or person is capable of assuring this vast network of capabilities — the Department as a whole must assure our Global Information Grid (GIG). Everyone who uses, builds, operates, researches, develops, tests, and explores information technology is responsible for IA. Everyone must be aware of his or her role in assuring the nation's information. A clear and coherent policy framework is required to achieve that awareness and the synergy it creates. The Department's transformation to Network-Centric Operations is most prevailing policy driver. For IA, net-centricity is a transformation of what we do, because the way we protect information and defend information systems and networks is fundamentally different in a globally interconnected world.

In October of last year DoD published its capstone directive on IA followed by a supporting instruction in March of this year. The directive establishes basic policy and assigns responsibilities to achieve IA through what we refer to as a 'Defense-in-Depth' approach that integrates the capabilities of technology, operations and personnel. The instruction implements policy by further assigning responsibilities and prescribing procedures for applying integrated, layered protection of DoD information systems and networks. These two documents establish the IA framework for the transformation from Platform-Centric to Network-Centric Operations. The new directive and instruction are comprehensive, focusing on the confidentiality, availability, integrity, authentication and non-repudiation of information; essentially all IA services not just the traditional confidentiality aspects.

These documents set the tone and lay the foundation for all remaining IA policies such as those for System Certification and Accreditation, Network Ports and Protocol Management, Computer Network Defense (CND), and CND Response Actions. They establish management boundaries and responsibilities at the Department level, the Component level, and the individual system level. They also organize information systems into 4 types¹ in order to better focus accountability for addressing IA during system development, during operations, in the acquisition of IT services, and in network interconnections.

The new policies also establish a banded risk model to help information and system owners determine appropriate target levels of confidentiality, availability, and integrity. These target levels are expressed as IA Controls, which address security best practices for general threats and system exposures, federal and DoD policy requirements, and IA interoperability across the GIG. The intent is to use these IA Controls as standard terms of reference for metrics and reporting. The Joint Staff has already taken a first step in that direction by cross-referencing them in the Joint Quarterly Readiness Review (JQRR) guidance, and we are working to make them the foundation of our FISMA (Federal Information Security Management Act) reporting. DoD's Operational Test and Evaluation directorate will test the controls during the conduct of 'Red Team' assessments of newly deployed systems.

As I mentioned earlier, our IA directive and instruction are the foundation of our IA policy framework. That framework is organized into 9 sub-categories (General; IA Certification & Accreditation; Security Management; Computer Network Defense; Interconnectivity / Multiple Security Levels; Network and Web; Assessments; Education, Training and Awareness, and Other IA (Integration)). The General sub-category

¹ The four types of information systems are:

Enclaves – operational networks and computing centers with IA focus on security management and administration

AIS Applications - IT acquisition or development initiatives with IA focus on building protection in

Outsourced IT-based processes - acquisition of IT services with IA focus good source selection factors and allocation of IA responsibilities between service provider and government users

Platform IT Interconnections – network connections of weapons systems and other platforms with embedded IT (e.g., medical systems, utilities systems) with the IA focus on managing connection risk

currently contains the IA directive and instruction I mentioned previously. A Handbook and Manual are in development. We have published policy for our core missions of Protect and Defend, policies that guide the Computer Network Defense mission. We also have policies in progress to support other goals and missions. We are making good progress in the formulation of policies that support multiple goals and missions such as Ports and Protocols Management, Interconnectivity, and Assessments. Formal policies covering Identity Management, Public Key Infrastructure, Public Key Enabling, and Biometrics are not as mature. However, strong acquisition programs and memo policies support these areas.

There will be major challenges in the maturation of the IA policy framework. Our DoD IA community is large and diverse, and IA is both pervasive and interdependent upon many other policies and processes—a particular challenge for the policy formulation process. There are, however, opportunities to improve the formulation process. We are examining ways to make the process more open, more visible, more collaborative, and, as a consequence, faster. A second challenge is the dissemination of new policy along with the vision and intent behind the policy. Published and draft versions of DoD IA policy are available online. We have also published Frequently Asked Questions and tutorials for the two foundation documents, and we are looking at ways to provide an online, web-based environment that helps users navigate through the IA policy library at the right level of readership – executive, manager, practitioner. A third challenge that we will continue to address is the integration of IA into related policies and programs. We have effort underway to work the integration of IA into the acquisition process to include designating IA as a Key Performance Parameter in major systems acquisition programs. We will be expanding that effort to also cover requirements generation. The last and perhaps most important challenge is IA policy change management and the effect of DoD IA policy changes on Combatant Command, Service and Agency implementing policies and programs.

DoD IA policy establishes top level who, what, and the procedural how. DoD has also developed and is implementing an Information Assurance (IA) Strategic Plan. The plan defines the Department's goals and strategic objectives for IA, providing a consistent, Department-wide approach to assuring our information. It was prepared through the cooperative efforts of the Combatant Commands, Services, and Agencies (C/S/As) and is intended to be a living document. We are aligning our investments and strategic initiatives to the objectives in the plan and are developing milestones and performance measures to gauge their success. All of this is done in close coordination with the Department's Global Information Grid architects, product and system developers, and acquisition executives. The Strategic Plan or roadmap has five major goal areas aligned to the technology, operations and personnel capabilities of our 'Defense-in-Depth' approach to IA. Each goal has supporting strategic objectives, sub-objectives, timelines and associated metrics. The goal areas are:

1. Protect Information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client (desktop), within the enclave (base network), at the enclave boundary (interface with global transport network), and within the computing environment (applications and operating systems), to ensure that all information has a level of trust commensurate with mission needs. The goal of the Global Information Grid is to allow information originating from anywhere on the network to be available throughout the network. Often the originator has little foreknowledge of who will use this information. Therefore, the new burden on IA is to ensure that all information is protectable. This means that all information can be protected from "end to end" and throughout its life cycle.

DoD has already invested in programs such as Public Key Infrastructure, Biometrics, and Common Access Control (CAC) Cards to support this goal. By the end of this year, we expect nearly all DoD personnel to be outfitted with a CAC card for identification and access to the network. However, more effort is needed to ensure that these tools are implemented throughout the DoD enterprise. DoD is focusing hard on the use of open standards and Extensible Markup Language for interoperability both within DoD and

with industry and the business community. The key is to do that securely. We are involved intimately with the rest of the Federal government in identification and identity management efforts. We want to insure that the mechanisms we use in our defense missions do not have to be duplicated in our interactions with the rest of government. Coalition, cross security-domain, and collaborative communications require "tagging" of people and information in order to provide agility for dynamic access control decisions. Our supporting protection infrastructures (Key Management Infrastructure, PKI, and network management systems) must have a higher level of assurance in order to provide an integrated systems security posture. Achieving this goal requires partnerships and combined efforts with other components of the security community; physical security, personnel security, and critical infrastructure protection.

2. Defend Systems and Networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense. DoD systems and networks are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and implementation of systems and networks across the enterprise. In addition, capabilities must be deployed to react and respond to internal as well as external threats and attacks.

3. Provide Situational Awareness/IA Command and Control (C2) integrating the IA posture into common operational pictures to provide a shared understanding among decision makers through decision tools that assist in the planning, execution and monitoring of coordinated actions. Combatant Commanders must have sufficient visibility of their networks, threats, and operations to gain a full awareness of their situation. The complex and interdependent nature of our networks and the demands of Network-Centric Warfare require shared awareness and understanding across the enterprise. The role of the IA community is to work closely with Combatant Commanders and key agencies in building the requirements for the Common Operational Picture and the Standing Joint Force Headquarters (SJFHQ). The DoD must have IA Situational Awareness and C2 requirements built in if it is to share information, process it

effectively, gain a shared understanding, and act in a synchronized fashion to respond in an effective and appropriate manner. This extends to other government and private sector partners as well as to our international allies to provide us a worldwide situational awareness critical to proactively defending our forces both at home and globally.

4. Transform and Enable IA Capabilities to develop and deliver dynamic IA capabilities and to improve inter and intra entity coordination (government to government, government to industry, and intra-defense) to reduce risk and increase return on investment. Network-Centric operations demand greater process agility and integration. As such, this goal focuses on improving the processes integral to developing and delivering IA capabilities supporting the transformation of the force. DoD's processes are generally designed to follow a cycle of deliberate planning, operations, and disengagement. Decision support processes are designed to function in a time-linear way. As a result, our responsiveness is often too slow or ill matched to the environment in which we now operate. The Network-Centric Warfare environment requires rethinking and innovation in how we reshape the processes of planning, programming, and resourcing in order to be responsive to ideas that take hold and become marketed in time frames faster than current processes can accommodate.

The ever-changing and evolving information technology industry stresses DoD's processes and challenges them to keep pace. Maintaining a competitive edge over our adversaries demands that we transform the mechanisms used to develop and deliver new and dynamic capabilities to become more responsive to ever-changing needs. Agility must be a goal that every process meets to maintain a competitive edge. Continuous improvement is mandated. This approach places great importance on harvesting and prioritizing ideas and the rapid development and deployment of concepts and capabilities to enable constant and continuous preparation, shaping, and execution of our responses to the environment.

5. Create an IA-Empowered Workforce that is trained, highly skilled, knowledgeable, and aware of its role in assuring information. Well-trained people are the cornerstone of any successful IA/IT program. Given today's threats against IT systems and networks, it is important that all personnel understand the critical role of IA within their daily work activities. In order to maintain a DoD workforce that is technologically sound, various programs must be instituted to support the IA mission (i.e., training and education, IA/IT awareness, and recruitment and retention initiatives). To create an IA-empowered workforce, there are three critical success factors: (1) a need for constant vigilance, (2) well-equipped IA/IT personnel, and (3) buy-in from key decision makers. The need for constant vigilance in information security and awareness is key to deterring threats and mitigating vulnerabilities. Establishing an IA/IT workforce that is equipped with the proper skill sets and tools allows the Department to create and implement value-added solutions that are agile and technologically advanced. We are also leveraging initiatives to create centers of academic excellence in our colleges and universities as well as IA scholarships with the goal to improve our recruitment and retention. Through efforts like these and our System and Security Administrator Certification Program, we will achieve this goal.

This Strategic Plan is the roadmap for DoD in assuring our information, and it serves as a guide for all Services and Agencies within the Department. At DoD's enterprise-wide IA conference last January, then NSC member Howard Schmidt while describing the National Strategy to Secure Cyberspace pointed to the common themes and complementary nature of both our documents. We will continue to review our vision, goals, and objectives for relevancy, currency, and applicability. Implementing the IA Strategic Plan requires the involvement of all Combatant Commands, Services, and Agencies and will require the continued support and commitment of DoD leadership, to include the IA Senior Leadership Group (senior IA leaders from the Department's Combatant Commands, Services, and Agencies), the DoD Chief Information Officer, and the Military Communications and Electronics Board (MCEB). Oversight of the implementation, reviews, and updates to the Strategic Plan falls to the IA Senior Steering

Group. My directorate will serve as the Strategic Management Office for the IA Strategic Plan, and a Goal Lead internal to my organization has been assigned to each of the five IA goals. The Plan, supported by our policy framework, is a dynamic roadmap designed to support Secretary Rumsfeld's transformational force.

While the Network-Centric transformation of national defense capabilities is the primary driver of DoD IA policy and our IA Strategic Plan, we must also address federal and statutory requirements. These requirements influence how we organize, interact, and manage. They also tell us that there are many consumers of information assurance management information – program analysts, budget analysts, auditors – who are not IA technical specialists. Our challenge in creating a management or command and control language for Information Assurance is to ensure that it is expansive enough to serve all audiences – military, technical, business management, and oversight.

The Federal Information Security Management Act of 2002 (FISMA) is perhaps the most influential statutory requirement for DoD with respect to IA. A strengthened version of the Government Information Security Reform (GISR) provisions of the FY 2001 Defense Authorization Act, it requires DoD as well as other agencies to ... provide information security protections...comply with information security standards... ensure information security management processes are integrated with agency strategic and operational planning processes...as well as numerous other responsibilities. The policies and strategic plan I described for you are our tools to meet those responsibilities. In both the FY2001 and FY2002 GISR reports to Congress, OMB mentioned areas where the Department excels. Our IA training program is, "the most comprehensive training program and processes of any Federal department or agency." The Department has a fully functional and effective incident response capability. Guidance and procedural frameworks for detecting, reporting, and sharing vulnerabilities are documented. In fact our incident and response center is an integral part of the Federal community's cyber warning network. The report also mentions that DoD has undertaken aggressive action to improve and expand its information assurance capabilities by implementing the Information Assurance Vulnerability Alert (IAVA) process to all Services and agencies;

ensuring timely distribution of effective computer security policies and procedures; and improving DOD business processes to ensure that all systems are protected. We are far from perfect, however, and are working diligently to improve our system certification and accreditation practices and the databases that help us track those certifications. That effort is more than an accounting drill. It is a comprehensive effort to get near real time visibility of our entire network, manage configuration enterprise wide, distribute changes and security patches, and perform consequence management when something effects the operation of our systems and networks.

The challenges we face are the same challenges found throughout government and industry. Those are the challenges we are addressing in our IA Strategic Plan. Do we have unique challenges? Yes, but they are not insurmountable. Size, global presence, dynamic technical and operational requirements all contribute to the complexity of our environment. But, we are adapting. We are making progress. We are managing the risk and managing it successfully across all of our National Security missions within DoD. That success is documented in our GISR, now FISMA reports as well as in our Annual IA report to Congress. Most important, however, it is reflected in our ability to act as an enabler, not an impediment, in the conduct of Network-Centric Operations in several theaters across the globe.

We have come to realize that we will never be able to achieve absolute protection of our information, systems and networks. However, we also realize that we can effectively mitigate the effects of challenges to the security of our information, systems and networks. We have created a robust Computer Network Defense capability within the Department, a capability that continues to evolve and transform itself in pace with the evolving and transforming threat.

IA is a journey, not a destination. That may be a hackneyed phrase but it accurately depicts The IA environment in DoD. All systems are legacy systems as soon as they go online. The demand for greater bandwidth, functionality, connectivity and other features is constantly expanding. That demand will be met. Our task within the Department is to

insure it is met securely. IA must be baked in and not spread on as an afterthought. We are stepping up to that challenge. DoD's IA community is intimately involved not only in the development of protective technologies for space-based laser, advanced fiber optic, and wireless transport networks but also in the development of end-to end IA architectures and technologies. From the labeling of information and people for controlled access to the security of enterprise computing environments, we are working now to ensure IA is baked in from both the protect and defense perspectives.

I appreciate the opportunity to appear before the Subcommittee and look forward to your continuing support on this very critical issue. Thank you.