

**Statement by
Robert G. Gorrie
Deputy Director
Defense-wide Information Assurance Program Office**

**Office of the Assistant Secretary of Defense for
Networks and Information Integration
and
DoD Chief Information Officer**

**Before The
Committee on Government Reform
Subcommittee on
Technology, Information Policy, Intergovernmental Relations and the Census
Hearing on
“Exploring Common Criteria: Can it Ensure that
the Federal Government Gets Needed Security in Software?”**

September 17, 2003

For Official Use Only
Until Release by the
Committee on Government Reform
U.S. House of Representatives

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 continue to make significant progress in our quest to secure and defend our computer networks. My testimony will highlight some efforts we have initiated with respect to the evaluation of Information Assurance (IA) and IA-enabled products.

Secretary Rumsfeld, in one of his initial statements before the House Appropriations Defense Subcommittee, identified six key transformational goals for the Department. One of those transformational goals is to leverage Information Technology (IT) to create a seamless, interoperable, network-centric environment. 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 IT 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 network 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 relationship, the Secretary identified protection of U.S. information networks from attack as another of the transformational goals.

Secretary Rumsfeld describes transformation as an ongoing process, not an event – 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 DoD transformation by providing the power of information to that leading edge. To bring power to the edge, he established the following goals: (1) develop a ubiquitous network environment, (2) populate the network 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 technology, operation, or person is capable of assuring or protecting the Department's vast networks and information. Everyone who uses, builds, operates, researches, develops and tests IT is responsible for assuring the Department's information and information infrastructure. A clear and coherent policy framework is required to ensure that individuals and organizations are aware of their responsibilities, and the Department's transformation to Network-Centric Operations is the framework we use to clearly define the "whys" and "hows" for such policy. 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 2002, the Department published its capstone IA policy, DoD Directive 8500.1, "Information Assurance" followed in February the following year by amplifying policy in DoD Instruction 8500.2, "Information Assurance (IA) Implementation." The directive establishes basic policy and the instruction implements policy by further assigning responsibilities and prescribing procedures for applying integrated, layered protection of DoD information systems and networks.

The new policies establish a 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 DoD Global Information Grid or 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 guidance, and we are working to make them the foundation of our Federal Information Security

Management Act (FISMA) reporting. DoD's Operational Test and Evaluation office will test the controls during the conduct of 'Red Team' assessments of newly deployed systems.

The DoD's IA strategies and policies are central to the Subcommittee's Common Criteria question. As I stated, no one single technology, operation, or person is capable of assuring DoD's vast global networks. The Common Criteria, the National Information Assurance Partnership (NIAP) evaluation program, the National and DoD policy addressing IA evaluations, and the evaluated products themselves are parts of an integrated DoD IA strategy. The technical strategy that underlies DoD Information Assurance is Defense-in-Depth, in which layers of defense are used to achieve a balanced overall Information Assurance posture. To take advantage of rapid advances in information technology the Department maximizes the use of COTS and balances this with layered security.

Even with a solid Defense-in-Depth strategy in place, a fundamental precept is our maintenance of confidence in the security and trustworthiness of the products we use to implement that strategy. New vulnerabilities in the equipment we use, both government and COTS, are identified daily. Through the Department's IA Vulnerability Alert (IAVA) process and attendant alerts, bulletins, and technical advisories, users are made aware of the vulnerabilities and associated fixes. The IAVA process serves us well, minimizing the disruption of DoD networks during recent cyber incidents that caused widespread disruption elsewhere. The IAVA process has also highlighted the alarming rise in the number of vulnerabilities, the risk they present, and the cost associated with their remediation. Although we continue to improve the efficiency and effectiveness of the IAVA process, unless we take proactive measures to reduce the number of vulnerabilities in our systems and networks, our ability to respond will begin to degrade.

The Chairman of the Joint Chiefs of Staff champions the concept of "born joint" as a way of expressing the need for built-in, seamless interoperability in new war fighting systems. Similarly, new IT products and systems must be 'born secure'; designed, tested, and validated against specific security requirements. The concept of 'born secure' combined with an aggressive vulnerability management program incorporating the IAVA process,

gives us the ability to proactively reduce our exposure to known vulnerabilities and maintain the capacity to respond to evolving vulnerabilities.

To help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established a program under the NIAP to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security, or Common Criteria Scheme in abbreviated form, is a partnership between the public and private sectors.

NIAP maintains a Validated Products List containing all IT products successfully completing evaluation and validation under the Common Criteria scheme. The validated products list also includes those products successfully completing similar processes under the schemes of authorized signatories to the Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security. One of the challenges is to produce a full suite of U.S. security requirements, or protection profiles, required for industry to evaluate their products. The IA community is working hard to keep pace with the unique security requirements of constantly evolving and new IT by developing new protection profiles in collaboration with industry and academia.

Timeliness is a key performance parameter. The government must rapidly integrate secure cutting-edge products into its IT enterprise and industry must meet time-to-market requirements. We cannot still be evaluating Version 4.0 of a product when Version 6.0 is on the market. In the aftermath of the events of September 11, NIST and NSA accelerated the protection profile development process and recently announced a new collaborative effort to produce comprehensive security requirements and security specifications for key technologies that will be used to build more secure systems for our Federal Agencies. These security requirements and security specifications will be developed with significant industry involvement. Protection profiles in key technology areas such as operating systems, firewalls, smart cards, biometrics devices, database systems, public key infrastructure

components, network devices, virtual private networks, intrusion detection systems, and web browsers will be the primary focus of this high priority project. With defined product security requirements and specifications, a defined and efficient product evaluation process and most important, a strong partnership with industry we will be able to populate the Validated Products List with up to date and secure IA and IA-enabled products.

Although no product will ever be totally secure, we can incorporate security into their design and through comprehensive security test and evaluation gain a reasonable sense of the risk we assume when we use them. However, for that concept to become a reality, it must be codified in policy and enforced in practice. In January 2000, the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee, issued its National Information Assurance Acquisition Policy. That policy directs, “by 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products shall be limited only to those which have been evaluated and validated in accordance with criteria, schemes, or programs of the Common Criteria, the National Information Assurance Partnership (NIAP) evaluation and validation program, and the Federal Information Processing Standards (FIPS) validation program.”

DoD policy goes further than the National policy, requiring the evaluation of all IA and IA-enabled products, not just those used in National Security Systems. Department acquisition policy includes references to the mandates of CNSS and DoD IA policy to insure IA is a key element of all acquisitions. The combination of the CNSS and DoD policies, the Common Criteria IA validation scheme, and the development of Protection Profiles in key IT areas is the foundation for ‘born secure’ IT.

Internal to the Department, Services and Agencies have published supporting service/agency specific policy for the evaluation of IA and IA-enabled products. We have an aggressive NIAP awareness campaign within the department. We also have enacted controls to monitor and enforce compliance with policy. The first conversations between a vendor and user often center on the requirement and timeline for NIAP evaluation.

While vendors' drivers are primarily product cost, functionality and time-to-market, security has become as significant consideration. Recently, the nation's largest vendors have pledged to make security a priority. For example, on Jan 15, 2002, Bill Gates released an email stating Microsoft's highest priority. *"Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing."* Microsoft's decision and the decision of many other vendors to focus on security are based on thorough business case analyses. None can afford the continued cost of the race against the "penetrate and patch" approach to deal with latent vulnerabilities in software packages. Simply, the economic cost of this "penetrate and patch" approach is enormous and does not result in a higher level of security. Sound software engineering practices, like those tested in a NIAP evaluation, are an essential element in the elimination of vulnerabilities and critical to the reduction of post deployment patching.

Still, there remains the cost of evaluation and the time of evaluation. Both are functions of the complexity of a product, the level of evaluation, and the quality of a vendor's product and preparation for evaluation. The amount of testing required in evaluation is directly proportional to product complexity and evaluation level. The amount of testing relates directly to time and cost. A quality product will not require much repeat testing. Products that get into a test, fail, fix, and test cycle incur additional costs not only for testing but also for product modification.

Some vendors, especially small vendors, are concerned about the cost and time of evaluation regardless of product complexity and evaluation level. During the development of DoD policy, we met with small businesses, individually and in multi-vendor forms. Based on their input, we developed policy that attempts to remedy some of their concerns, specifically the concern over the investment in evaluation without knowing if there would be a return on that investment. e.g., DoD policy states, "...products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the

contract.” Vendors can now enter competition and if selected realize a return on their evaluation investment. Other modifications were also made to policy based on consultation with industry.

Questions have been raised about the efficacy of the end-to-end evaluation process itself and the extensibility of the process to the entire Federal government and civil community beyond National Security System users. The evaluation process does what it was designed to do. It provides standardized evaluation reports that help us make informed risk management decisions with respect to the security of our networks and systems. Expectations of evaluated products should not exceed what the evaluations are designed to provide. If a protection profile at a particular evaluation level does not call for the evaluation of some security functionality, it will not be evaluated. The type of testing that uncovers vulnerabilities like the buffer overflows exploited by some of the recent worms can be done by the NIAP laboratories and will be done if required. The depth of evaluation depends on how much time and money we are willing to pay as well as how much risk we are willing to accept. Evaluations do not guarantee security. The security comes from sound system security engineering, the combination of technologies, operations and people.

The President’s recent “National Strategy to Secure Cyberspace” requires a comprehensive review of NIAP to examine its effectiveness and expansion potential. We are conducting that review in collaboration with the Department of Homeland Security (DHS) to support the President’s strategy as well as the need for the evaluation process to keep pace with technology and DoD’s overall transformation efforts. DoD is also investigating the issue of Software Assurance with respect to all software, not just IA and IA-enabled products, again working with DHS. Our review of NIAP will help us improve the process and incorporate changes that will give us more confidence in the security of our IA and IA-enabled products.

The challenges we face are the same challenges found throughout government and industry – challenges we are addressing in our IA Strategic Plan. Does DoD have unique challenges – yes, but they are not insurmountable. Size, global presence, dynamic technical and operational requirements all contribute to the complexity of the Department’s environment.

But, DoD is making progress, managing the risk successfully across all of our National Security and Defense missions. That success is documented in our FISMA reports as well as in our Annual IA report to Congress. Most importantly, 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 trite phrase but it accurately depicts the IA environment in DoD. Most systems are legacy systems as soon as they go online. The demand for greater bandwidth, functionality, connectivity and other features is constantly expanding. The IA challenge within the Department is to insure it is met securely. IA must be 'baked in' and not 'spread on' as an afterthought. DoD and the DIAP 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' and products are 'born secure' 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.