

NOT FOR PUBLICATION UNTIL RELEASED BY THE  
GOVERNMENT REFORM SUBCOMMITTEE, TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

WRITTEN STATEMENT OF

MS DAWN MEYERRIECKS, CHIEF TECHNOLOGY OFFICER, DEFENSE  
INFORMATION SYSTEMS AGENCY

BEFORE THE  
GOVERNMENT REFORM SUBCOMMITTEE ON TECHNOLOGY, INFORMATION  
POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

WEDNESDAY  
2 JUNE 2004

CLEARED  
FOR OPEN PUBLICATION

MAY 25 2004 8

SECURITY REVIEW  
DEPARTMENT OF DEFENSE

NOT FOR PUBLICATION UNTIL RELEASED BY THE  
GOVERNMENT REFORM SUBCOMMITTEE, TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

DFOLSR 04-C-0922

**STATEMENT FOR THE RECORD**

**MS DAWN MEYERRIECKS  
DEFENSE INFORMATION SYSTEMS AGENCY  
BEFORE  
GOVERNMENT REFORM COMMITTEE  
TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL  
RELATIONS AND THE CENSUS  
SUBCOMMITTEE**

*Prepared Statement of Ms Dawn Meyerriecks, Chief Technology Officer, Defense Information Systems Agency, before the Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Washington, D.C., June 2, 2004.*

Thank you, Mr. Chairman and members of the Subcommittee, for this opportunity to testify before your Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census on the subject of Information Security – Vulnerability Management Strategies and Technology. I am Dawn Meyerriecks, Chief Technology Officer for the Defense Information Systems Agency (DISA).

As Chief Technology Officer for the Defense Information Systems Agency, I, along with Lieutenant General Harry D. Raduege, Director of DISA, am responsible for guiding the Agency's technical direction to execute the Global Information Grid (GIG) Initiative. I am responsible for the identification, evaluation, and incorporation of technology into the Agency's business processes and products.

DISA is a combat support agency. DISA is responsible for building, operating and protecting joint command, control, communications, and computer capabilities to help catalyze and sustain the Department of Defense's (DoD) transformation from platform-centric to network-centric operations. Key to this transformation is the foundation infrastructure known as the Global Information Grid (GIG).

The GIG is a network of unprecedented complexity. It crosses organizational boundaries within DoD and many outside of DoD. The GIG is composed of a huge variety of computer, software, and communications technologies. The responsibility for managing these technologies is currently fragmented across many DoD organizations and extends to many of our commercial partners. In order to better align the management of the GIG with DoD operational priorities, and to improve management and accountability, DoD is implementing a concept called NetOps, or network operations. One facet of NetOps is the development of a clear chain of command for the GIG, starting with U.S. Strategic Command. Accountability and reporting for vulnerability management in the DoD will be handled in this chain.

Assuring the availability of the GIG, and assuring the execution of missions that depend on the GIG are the key principles of DoD information assurance. DISA believes that security in the GIG can only be built and maintained by a broad DoD effort to design security into the GIG; to maintain this security as conditions change; to train our people to perform secure operation of the GIG; and then to operate the GIG in a way that ensures mission effectiveness for the DoD, even in the face of cyber attack.

DoD resists cyber attack by employing a multi-layered defense strategy. Core to this strategy is the notion of vulnerability management. Vulnerability management is a process that includes the development of DoD standards for secure configuration of devices in the GIG; the deployment of these configurations to every GIG component; the development and deployment of modified configurations, including patches, as new vulnerabilities and attacks are discovered and developed; and the local and global auditing and reporting of compliance with the DoD configuration standards.

DISA has coordination, strategy development, technology acquisition and fielding, auditing, and operations roles in vulnerability management. I'll talk about the DISA operations roles first, then talk about some of our technology acquisition and deployment efforts, and conclude with our auditing and verification efforts.

The DISA Global Network Operations and Security Center (GNOSC) performs and oversees the essential network and systems management of the GIG on a 24 by 7, 365-day a year basis, to ensure sustained and responsive, integrated network operations. The GNOSC is the single network operations center in DoD with a composite view of unclassified and classified global voice, data, and video communications used for command and control. Its primary mission is to direct, manage, control, monitor, protect, and report on essential elements and applications that comprise the GIG.

The DoD Computer Emergency Response Team (DoD-CERT) is charged with the global analysis of real or potential network security threats to the GIG. In partnership with the GNOSC, the DoD-CERT protects, defends, and restores the integrity and availability of the essential elements and applications that comprise the GIG under the full spectrum of conflict. An important vulnerability management role of the DoD-CERT is to monitor and research emerging vulnerabilities and attacks. When necessary, the DoD-CERT alerts all in DoD of the need to react, often by changing the standard configuration of a device. These alerts are called Information Assurance Vulnerability Alerts (IAVA) and have been issued since 1998. I will talk a bit more about IAVA later in my testimony.

The GNOSC and DoD-CERT provide primary support to the Joint Task Force-Computer Network Operations (JTF-CNO), a component of U.S. Strategic Command. As part of its larger DoD NetOps mission, the JTF-CNO oversees, coordinates, and directs information

assurance operations throughout the Department. Since the late 1990's the JTF-CNO has successfully defended DoD networks, thus ensuring the continuity of DoD operations in the face of computer intruders, viruses, and worms. The JTF-CNO's role in vulnerability management includes oversight of the IAVA process, and the collection and reporting of statistics on how well DoD organizations are doing in deploying and maintaining secure configurations.

Now I'd like to talk about DISA's efforts to develop the right, secure configurations for DoD, and our efforts to deploy technology that makes the complete cycle of vulnerability management more certain.

The innermost layer of our DoD cyber defenses is the computer itself. Ensuring each computer is configured securely and that each stays configured securely as conditions change seems like a simple problem, but it has been a tough one to solve for both DoD and industry. Many factors contribute to the complexity of this goal. These include: the intricacies of configuring a modern operating system securely; the difficulty in knowing that once configured, it is configured correctly; the sheer volume of new vulnerabilities in many operating systems; the increasing numbers of systems that need to be maintained; and the difficulty in updating and verifying the security of each of these machines in response to each new vulnerability. To help emphasize this point, there are currently more than 6,000 unique vulnerabilities listed in the Common Vulnerabilities and Exposures dictionary, the industry-accepted list of standard names for vulnerabilities that is maintained by the MITRE Corporation.

Despite these complexities, the first step on the path is clear: define secure configurations for DoD computers. Today's operating systems and applications are more flexible than ever, making the configuration possibilities practically infinite. The good news is that we have had success with innovative government and industry partnerships in developing

best practices in operating system and application configuration. An example is the partnership among DISA; the National Security Agency; the non-profit Center for Internet Security (CIS); the General Services Administration; the National Institute of Standards and Technology; Microsoft; and the Systems, Audit, Network, and Security Institute (generally known as the SANS Institute). This partnership resulted in consensus security configuration documents for Microsoft Windows that are published inside the DoD as Security Technical Implementation Guides (STIG), and are also published by NIST and by the CIS. Commercial Microsoft Windows systems administration training is now available that teaches to the standards defined in these guides, and finally, some major computer vendors have indicated interest in shipping computers pre-installed with these configurations and at least one is doing so. Since configuring a system to the DoD standard can be labor intensive and prone to error, the potential benefits to the Department are significant if vendors deliver products already properly configured.

Through similar collaborative processes, we have developed guides for every prevalent operating system and major application in use in the DoD; many are also applicable to the rest of the federal government. These community processes have laid the groundwork; we now have an established community consensus on operationally stable and secure configuration baselines.

The next step is to deploy these configurations everywhere in the Department. Currently we depend primarily on configuration by system administrators. This can be slow and prone to error, even when the system administrator has tools to help push clones of properly configured software out to many machines. Therefore, a DoD goal is to make deployment of the secure configurations more simple and reliable. One way is to urge software and hardware vendors to include the configurations when shipping products to the Department. We believe this is ultimately a large part of the answer to the problem of initial configuration of machines to proper

standards.

Another aid to the configuration of machines to the DoD standard is a DISA-developed product known as the Gold Disk, which is based on the standard configuration guidance. This government-developed product is intended to help system administrators determine the configuration of a computer and then help them automatically fix most configuration vulnerabilities. In calendar year 2003, we provided this technology to DoD for key Windows operating system versions and we are developing versions for some UNIX environments.

In a perfect world, we would be finished once we had the machines configured properly. However, with systems development and the installation of new systems and software, our infrastructure and systems are constantly changing. With change come new opportunities for our enemies to exploit our vulnerabilities. More importantly, with the worldwide usage and sheer complexity of common operating systems and applications, developers, users, researchers, and hackers frequently discover vulnerabilities. As each new vulnerability is identified, software vendors mount a rapid effort to understand the ramifications of the vulnerability and to develop a fix that removes or at least minimizes the vulnerability. Often, the vendors issue a short-term fix in the form of a patch to their existing software and then incorporate a design change in later versions of their software. However, no matter who first identifies a new vulnerability, the information about the vulnerability often becomes widely known in a matter of days. Therefore, a critical component of vulnerability management in DoD is to keep operating systems and application configurations up-to-date with the latest vulnerability patches as they are released. The challenge we face is not only to counter future attacks through installed defenses, but also to develop processes and tools to maintain the secure state of our systems, both as a matter of course and as new threats emerge.

As mentioned earlier, DoD has implemented a process called IAVA to mandate the application of these short-term fixes for software and configurations when a significant threat to DoD missions exists. The IAVA process requires the Combatant Commanders, Services, Defense Agencies, and Field Activities to update configurations to incorporate the new patches or to take other vulnerability remediation actions directed by the DoD-CERT and to report their compliance, so the JTF-CNO can determine overall DoD risk.

Application of patches or other configuration changes to many machines quickly is the crux of the vulnerability management problem. DoD has not fully solved this part of the problem, but we have taken significant steps to make configuration change easier and more certain. DISA has established a distribution system for the dissemination of security relevant patches throughout the DoD. Patch repositories and anti-virus distribution servers are available on the classified and unclassified GIG networks. These repositories enhance DoD's ability to protect against newly announced vulnerabilities because we are no longer competing with the entire Internet community for access to vendor-released patches. DoD users have exclusive access to the repositories, thus speeding up the overall response. From this foundation, we have established DoD Software Update Service (SUS) Servers on the unclassified and classified networks, for the Microsoft baselines. These SUS Servers provide DoD system administrators with automatic notification, and if desired, automated download of significant Microsoft security updates. We have ongoing efforts to improve these services by ensuring that patch and antivirus servers are available in places with limited bandwidth, and by ensuring that patches are available from vendors, even though the Internet may be unavailable.

The Gold Disk is intended to help here as well. Updates of the Gold Disk are provided when new vulnerability information changes the standard DoD configuration. The Gold Disk is

then available, either via CD ROM or via download on all DoD networks, to help system administrators update previously configured computers.

Each of the capabilities described above is helping to make compliance actions easier and faster. However, Commands that own and manage significant numbers of computers can still have a tough time understanding whether each computer is configured properly, and whether patches mandated by IAVAs have been installed everywhere. DISA has several efforts to help administrators and Commands understand how well they are doing to comply with the standard configurations and updates mandated by IAVAs. In addition to the system auditing tools contained in the Gold Disk, each month DISA produces scanning scripts and configuration files for popular configuration scanning tools. These are available on all DoD networks and are intended to help a system or security administrator understand how well each machine conforms to the DoD standard configurations and whether all appropriate patches are applied. In addition to helping system administrators, these tools also help provide more accurate vulnerability management reporting and accountability. DISA also provides the DoD-wide means of reporting vulnerability remediation compliance.

Our major new technology initiative is the U.S. Strategic Command chartered effort to acquire DoD-wide licenses for commercial tools to help take inventory, and then detect and resolve vulnerabilities. Through the Information Assurance/Computer Network Defense Tools Steering Group, the Combatant Commanders, Services, and Defense Agencies have engaged to support consistency in implementation and use of these tools. This effort has now moved to the stages of a DISA-led acquisition, currently underway. This capability will build upon DISA's current program of providing scripts compatible with the vulnerability scanning tools already purchased and used throughout the Department. It will also provide a more comprehensive

deployment and more consistency in the application of remediation actions throughout the Department. We expect award of a DoD-enterprise scanning tool license this summer, with a remediation tool license in early fall.

As good as the supporting technologies, commercially available products, and implementing policies are, there are significant personnel components to this problem as well. Legacy environments; lack of vendor support for some still operational product lines; user and systems administrator training; and competing priorities for scarce resources require further focus. The DoD Certification and Accreditation process is just one step in providing this focus. Augmenting certification and accreditation and the regular use of vulnerability management tools, with a regular verification and support program, has helped to improve the DoD's security posture. DISA executes a robust verification program focusing on high-risk sites, such as the Combatant Commander networks and the classified networks. These programs, known as the System Readiness Reviews and Information Assurance Readiness Reviews are designed to look at the configuration and patch management programs within an organization; the overall security posture of their networks; their conformance with the STIGs and overall defense-in-depth principles; and are augmented with a traditional security review that considers continuity of operations, physical, and personnel security. DISA executes more than 120 of these reviews a year and has set standards for the military services to follow in order to expand the number of support visits, because more are necessary.

The Department as a whole has come a long way toward executing a meaningful vulnerability management program. There is still much work to do, not just in the sustaining base environment, but also in the highly dynamic operational commands where machines are continuously coming and going. Operations ENDURING FREEDOM and IRAQI FREEDOM

have driven home the challenges of operating information technology in the tactical environment, where access to commercial tools, to support, and to the time necessary to manage configurations are all very limited. We will continue to ensure that DoD and DISA efforts properly focus on the unique problems of our deployed warfighters.

Despite all of the good work, commercial product support, technology solutions, and leadership focus, nothing is fool proof. A configuration and patch management program must be implemented as a part of a robust and far-reaching Defense-In-Depth program. It is this program that enables the other work and serves to mitigate the remaining risks. Implementation of defense-in-depth includes: establishment of a secure DoD perimeter; maintenance of the security of the networks and transport infrastructure, including the routing and naming infrastructures; deployment of a secure, classified command and control network; and implementation of “demilitarized zones” for separating our internal Department computing from that of our partners, our allies, and the Internet. It is this secure environment, operated as part of overall DoD warfighting via NetOps, that is vital to DoD reliance on the GIG.

Mr. Chairman, members of the subcommittee, again, thank-you for the opportunity to appear before your subcommittee.