

**Statement by
Amit Yoran
Director, National Cyber Security Division, Office of Infrastructure Protection
U.S. Department of Homeland Security
“Information Security – Vulnerability Management Strategies and Technology”

Before the Subcommittee on Technology, Information Policy, Intergovernmental
Relations, and the Census
Committee on Government Reform
U.S. House of Representatives
June 2, 2004**

Good afternoon, Chairman Putnam and distinguished Members of the Subcommittee. My name is Amit Yoran, and I am Director of the National Cyber Security Division of the Office of Infrastructure Protection in the Department of Homeland Security’s (DHS) Information Analysis and Infrastructure Protection Directorate. As we approach the National Cyber Security Division’s one-year anniversary, I am pleased to have an opportunity to appear before the committee again to discuss “Information Security – Vulnerability Management Strategies and Technology.” In the National Cyber Security Division (NCSA) of DHS, we have designed and implemented our programs to execute against various key cyber security issues for the Nation, including those laid out in the *National Strategy to Secure Cyberspace* (“the Strategy”). Vulnerability management, reduction, and assessment are an integral part of all aspects of our strategy, and span across all program areas within the Office of Infrastructure Protection and the NCSA. Our initiatives are focused on the areas of incident management, our on-going collaboration with the public and private sectors, software assurance, and vulnerability assessment. As the focal point for the public and private sectors on cyber security issues, we work closely with our interagency colleagues and private sector partners to address these critical components of the mandate to increase our Nation’s cyber security and improve our ability to mitigate vulnerabilities to the greatest extent possible.

Introduction

The National Cyber Security Division (NCSA) was created in June 2003 to serve as a national focal point for the public and private sectors to address cyber security issues. NCSA is charged with coordinating the implementation of the *National Strategy to Secure Cyberspace* released by the President in February 2003. Since our creation, we have been evaluating and securing our areas of greatest vulnerability, in partnership with private industry.

DHS is working closely with our partners in the federal government, the private sector, and academia on a variety of programs. DHS recognizes that each entity may

bring unique capabilities, responsibilities, and/or authorities to bear on cyber security issues. We recognize that the challenge of securing cyberspace is vast and complex, that threats are multi-faceted and global in nature, and that our strengths – and our vulnerabilities – lie in our interdependencies. Further, the cyber environment in which the world operates is constantly changing. We recognize that information sharing and coordination are crucial to improving our overall national and economic security. Cognizant of these realities, our cyber security initiatives are designed to address each of the priorities set forth in the *National Strategy to Secure Cyberspace* (“the Strategy”):

- Priority I: A National Cyberspace Security Response System
- Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program
- Priority III: A National Cyberspace Security Awareness and Training Program
- Priority IV: Securing Government’s Cyberspace
- Priority V: National Security and International Cyberspace Security Cooperation

Our cyber security programs address each of these priorities and are beginning to improve our ability to manage vulnerabilities and incidents.

Vulnerability Management

The highly interconnected and interdependent digital economy in which we live and work today presents many challenges to managing information system vulnerabilities in all spectrums of the Nation including: government, large and small companies, academia, and even our private homes. The proliferation of complex information systems and the speed with which information flows today present great challenges for developing and coordinating programs to manage those vulnerabilities on the one hand, while also disseminating the appropriate information to those who need it, on the other. NCSA has initiated several programs to coordinate with various stakeholders, manage collaborative efforts, and address the diverse owner, operator, and user communities.

Incident Management

A major element of successful vulnerability management is incident management that includes a 24/7 incident management capability and the ability to know what to do when vulnerabilities are identified. Successful incident management also requires strong information sharing, communication, and coordination capabilities. DHS has implemented several initiatives aimed at addressing these different aspects of incident management.

Priority IV of the Strategy gives DHS the responsibility for securing government’s cyberspace. The U.S. Government has been actively engaged in assessing our preparedness and processes for responding to cyber incidents. In October of 2003, DHS participated in the first national cyber-focused exercise, called “Livewire,” which

provided a baseline for the federal government incident response capability and communication paths. Livewire also directly supported the creation of the Cyber Interagency Incident Management Group (Cyber IIMG), which was developed to improve response procedures and capabilities across government agencies. The Cyber IIMG coordinates intra-governmental preparedness and operations to respond to, and recover from, cyber incidents and attacks. The group brings together senior officials from DHS, the White House, the National Security Council, Homeland Security Council, OMB, law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security capabilities. The collaboration of these agency officials provides an improved capability to analyze and coordinate a national level response to incidents that may impact cyber assets. In addition to the ability to focus portions of their agencies' resources, they possess the necessary statutory authority to take decisive actions in response to incidents. The Cyber IIMG meets on a regular basis to address cyber incident coordination in general and identifies specific areas of concern to focus on at each meeting.

In addition to the coordination of senior management in the Cyber IIMG, DHS has also established the Government Forum of Incident Response and Security Teams (GFIRST), a consortium of federal response and information security teams working together to bolster government-wide incident response capabilities. This group provides a forum for security-focused technologists to communicate with a trusted set of peers responsible for protecting the government-owned and operated elements of the Nation's critical infrastructure. GFIRST promotes cooperation among the full range of federal agencies, including defense, civilian, intelligence, and law enforcement. We are already seeing the benefits of both the Cyber IIMG and GFIRST in improving communication and coordination among government agencies toward incident preparedness and response efforts.

DHS, in coordination with the White House and other federal agencies, has been working to provide mechanisms for improving vulnerability management and incident response that are crucial to protecting the Nation from a variety of vulnerabilities and attacks. DHS is developing a National Response Plan (NRP) that will include a Cyber Annex outlining the Government's processes for responding to a cyber attack or incident. The NCSD is developing the Cyber Annex to ensure that there are robust, reliable and efficient mechanisms for managing national level cyber incidents.

Congress also contributed greatly to the impetus and ability of federal agencies to protect their information infrastructure by passing the Federal Information Security Management Act of 2002 (FISMA). FISMA has been a key component in vulnerability mitigation and cyber preparedness by providing a framework for enhancing the effectiveness of information security and vulnerability management in the federal government. That framework has become a very visible federal agency information security benchmark, and as such, it has served to accelerate agencies' deployment of automated, enterprise-wide security assessment and security policy enforcement tools as well as threat and vulnerability management tools. FISMA also calls for the operation of a central Federal information security incident center. The Federal Computer Incident

Response Center (FedCIRC) program fulfilled the functions specified under FISMA and today, those functions are fully supported and integrated into NCSO watch operations. NCSO continues to maintain close coordination with the Office of Management and Budget (OMB) on cyber events that may impact the Federal government. DHS is a strong advocate of FISMA as an important, cohesive platform to secure government cyberspace.

Aside from our government-focused initiatives, DHS established the U.S. Computer Emergency Readiness Team (US-CERT) as its overall cyber security operational entity. US-CERT represents a partnership between NCSO and the public and private sectors, the founding partnership of which is between the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University. US-CERT provides a national coordination center that links public and private readiness and response capabilities to facilitate information sharing across all infrastructure sectors and helps to protect our Nation's cyber infrastructure. The overarching objective of US-CERT is to facilitate and implement a systematic readiness, coordination, and response mechanism to address cyber incidents and attacks across the United States, as well as to mitigate the cyber consequences of physical attacks.

The National Cyber Alert System (NCAS), launched by US-CERT in January of this year, is an important mechanism for vulnerability and incident management and warning. The NCAS is an operational system that delivers targeted, timely, and actionable information to Americans to allow them to secure their computer systems. Information provided by the system is designed to be understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. The NCAS provides general guidance for users and the ability to reach millions of users at once. The information NCAS provides is crucial to helping Americans take appropriate preventative measures against vulnerabilities to protect their computers.

When US-CERT has vendor-specific vulnerability or threat information rather than more general information typically sent through the NCAS, we communicate directly with the individual company when possible. The recent Cisco vulnerability is an important example of how we communicated – and collaborated – with the private sector on a vendor-specific vulnerability. US-CERT was notified by Cisco Corporation that there was a vulnerability in the Cisco Internetwork Operating System (IOS) implementation of the Simple Network Management Protocol (SNMP). This vulnerability affected many versions of the IOS and could have resulted in a sustained denial of service (DoS) condition if it had been exploited. Cisco representatives requested US-CERT assistance in providing the broadest possible dissemination of information concerning this vulnerability. The US-CERT incident management team was notified immediately and began efforts to coordinate notification of this issue. The US-CERT issued a Technical Cyber Security Alert using the NCAS and, utilizing the HSIN (Homeland Security Information Network)/US-CERT Portal, notified many cyber security communities, including the federal Chief Information Security Officers, the Information Sharing and Analysis Centers (ISACs), and critical infrastructure owners and operators, of the emergence of this new vulnerability. The ability to communicate with

specific companies in such cases to manage the vulnerability and the subsequent mitigation efforts is crucial and is one of the key drivers behind the creation of the US-CERT Partner Program.

The US-CERT Partner Program

DHS is currently working closely with the private sector to develop a comprehensive operational partner program to increase the Nation's cyber security. The US-CERT Partner Program will establish a formal collaboration mechanism between DHS, other government entities, academic institutions, and the private sector. This program will focus on partnerships between the public and private sectors for the purpose of improving national situational awareness with regard to cyber security and will coordinate cyber security across Federal, State, Local government, academia, and private industry. The Partner Program will be the cornerstone of national cyber security coordination for preparedness, analysis, warning, and response efforts across the public and private sectors to help ensure the cyber security of our national critical infrastructures and the Internet. Program partners will include the spectrum of the critical infrastructure sectors (including the Information Sharing and Analysis Centers (ISACs), industry associations, etc.), and the organizations that support these sectors from the private and public sectors, the research community, and academia.

The mission of the US-CERT Partner Program is to bring about measurable improvement in the Nation's ability to prepare for, recognize, respond to, and recover from cyber security incidents. In order to carry out this mission, the US-CERT Partner Program's objectives are to:

- Share information to prevent, predict, detect, and respond to cyber threats and vulnerabilities;
- Increase emphasis on improving the cyber security of our Nation's critical infrastructures;
- Provide actionable identification, analysis, and warning of cyber vulnerabilities, malicious code, exploits, and viruses to member partners;
- Improve cyber event response coordination within and between public and private sectors;
- Ensure a secure and trusted forum to promote analysis and facilitate exchange; and
- Create an effective forum to demonstrate national commitment to cyber security.

In order to provide actionable identification, analysis, and warning of cyber vulnerabilities, malicious code, exploits, and viruses to member partners, the US-CERT Partner Program will create a mechanism to collect, analyze, remediate, and disseminate information pertaining to the protection of our Nation's critical infrastructures, including vulnerabilities. Partners will commit to take steps to increase our overall cyber security preparedness, and our collaborative efforts will lead to improved vulnerability

management and incident response, and thus increased national and organizational cyber security.

Software Assurance

Another facet of successful vulnerability management is the importance of addressing and reducing vulnerabilities from the beginning. Thus, software development and assurance is a fundamental area of focus for DHS and for the public-private partnership.

The NCSA is taking a proactive approach to software assurance by examining problems such as flaws, bugs, and backdoors. Additionally, the NCSA is examining ways to improve the effectiveness, reliability, and risk of patches and software configuration. By addressing the root problems of current software development, we can eliminate vulnerabilities before products and application systems are deployed.

The NCSA recognizes the importance of creating more robust software security so that all users can continue to derive value from current and future software products. DHS is developing a program plan to work closely with the private sector, academia, and other government agencies to produce better quality and more secure software. DHS is evaluating the software development lifecycle, including people, process, procedures, and technology to implement a collaborative effort to mitigate risks and assure software integrity.

- **People** – Focuses on software developers (includes education and training) and users
- **Processes** – Focuses on developing best practices and practical guidelines for the development of secure software and associated standards, specifications, acquisition language
- **Technology** – Focuses on software evaluation tools

This comprehensive approach is consistent with recommendations from the Security Across the Software Development Lifecycle Task Force of the Cyber Security Partnership formed in connection with the National Cyber Security Summit that was co-sponsored by DHS and industry in December 2003. Through the work of the task force and individual corporate efforts, the private sector is seriously engaged in this effort. Companies are committing to reducing vulnerabilities by using state of the art engineering practices, standards, and processes throughout the cycle of creating their software. For example, a software vendor tells us that such enhanced development processes have resulted in a notable decline of vulnerabilities in some of their server software and a corresponding reduction in the number of patches for their users.

Furthermore, research and development (R&D) must play a significant part in enhancing cyber security for the future. The DHS's Science and Technology (S&T) Directorate has plans for R&D investments aimed at improving software assurance and code development, as part of programmatic activities that will be initiated later this fiscal

year. In addition, the S&T Directorate has initiated an effort aimed at supporting the creation of large-scale data sets for testing of network security technologies. These data sets are intended to support the university and industry R&D communities by improving research, development, and evaluation of alternative approaches to network security.

Technology

Chief information security officers play a vital role in vulnerability management for their organizations. As such, DHS established the Chief Information Security Officer Forum (CISO Forum) for the education and professional development, collaboration, and coordination venue for agencies' designated senior federal IT security executives. The CISO Forum provides a trusted venue for our government information security officers to collaborate and share effective practices, initiatives, capabilities, successes and challenges. In addition, the CISO Forum provides education on FISMA and leading edge security tools and methodologies – including encryption, authentication, shielding, configuration management, and intrusion detection. The education and interagency collaboration in the CISO Forum allows federal chief information security officers to continually improve vulnerability management in their respective agencies and departments and better secure federal systems.

We hear much about patch management as we look toward vulnerability mitigation possibilities. Since the Patch Authentication and Dissemination Capability (PADC) program was initiated in 2001, patch management technology has significantly surpassed the spartan capability of that time. In an effort to streamline its own efforts in this regard, the NCSO discontinued the PADC program. It was determined that the existing contract was too inflexible and financially constrained to affect necessary enhancement. Since the management, architecture, and resources of each agency vary, it is unlikely that a single solution will satisfy every need. Therefore, NCSO has engaged the CISO Forum to undertake an examination of agencies' needs, as well as the current state and future development of patch technology. A CISO Forum working group will study current patch technology and attempt to understand the common needs of agencies, in addition to how the patch management industry may assist in responding to sudden and potentially damaging exploitation of vulnerable software. Additionally, with the implementation of the National Cyber Alert System, discussed previously, US-CERT will fill the void of early notification of vulnerabilities that the PADC program provided. Patch management is necessary to address the vulnerabilities and incidents that occur due to today's software security limitations. DHS is striving for the proliferation of secure software for consumers and other customers through our software assurance programs and efforts with software developers. Until that time, however, effective patch management is a necessary objective.

Vulnerability Assessment

Comprehensive vulnerability assessment is another necessary aspect of vulnerability management. As part of the Critical Infrastructure Protection initiative

mandated under Homeland Security Presidential Directive 7 (HSPD-7), released by President Bush on December 17, 2003, the Department of Homeland Security is coordinating physical and cyber vulnerability assessments of critical infrastructures, working with sector specific agencies. Under HSPD-7, sector specific agencies have responsibility to identify critical assets, develop methodologies to assess vulnerabilities, and map those vulnerabilities to critical assets in a risk assessment analysis. DHS is responsible for the correlation, analysis, and trending of the information provided by those agencies. The NCSD, as the information technology (IT) sector specific lead agency, is responsible for identifying the critical assets and related vulnerabilities in the IT sector.

A fundamental goal of the National Critical Infrastructure Protection (CIP) Program is to identify and protect infrastructures that are deemed most “critical” in terms of national-level public health and safety, governance, economic and national security, and public confidence. The Department of Homeland Security (DHS) recognizes that such protection requires the cooperation and essential collaboration of federal agencies and departments, state and local governments, and the private sector. Accordingly, to achieve the overarching goal of protection, and to reduce vulnerabilities across the entire critical infrastructure – physical and cyber - DHS is coordinating the development of consistent, sustainable, effective, and measurable CIP programs across the federal, state, local, and private sector. DHS is coordinating with SSAs in developing their plans for implementing critical infrastructure protection (CIP) responsibilities required under Homeland Security Presidential Directive (HSPD) 7. These Sector-Specific Plans will be incorporated into the NIPP, called for under Paragraph 27 of HSPD-7.

After the initial assessment and determination of vulnerabilities by all sector specific agencies, a remediation plan will be developed within each sector specific agencies to address the vulnerabilities. DHS, NCSD will analyze the inputs and look for common vulnerabilities which can be addressed through long-term strategic initiatives. These efforts will vastly improve vulnerability mitigation and management in the 13 critical infrastructure sectors.

Conclusion

DHS has made great strides to implement a variety of programs and partnerships to help secure cyberspace. Vulnerability management is a critical area targeted by DHS in order to increase cyber security not only for today but also for the future, including comprehensive incident management initiatives, coordination with the private sector through the US-CERT Partner Program, software assurance and development programs, and cyber vulnerability assessments of the critical infrastructure sectors. In addition, we bring together key cyber security stakeholders together through various forums to address the technical and management issues in a collaborative way across the federal government, state and local governments, academia, and the private sector.

Thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.