Testimony of

Mr. Amit Yoran

February 24, 2004

Statement by
Amit Yoran, Director
National Cyber Security Division
Department of Homeland Security

Before the U.S. Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology, and Homeland Security
February 24, 2004

Thank you, Chairman Kyl, Senator Feinstein, and distinguished members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the important issue of cyber terrorism. I also welcome the chance to provide your Subcommittee with an update on the efforts of the Department of Homeland Security's National Cyber Security Division (NCSD) to defend our Nation against the menace of cyber threats.

The NCSD, established by the Department in June 2003, represents a crucial component of the Information Analysis and Infrastructure Protection (IAIP) Directorate. Under the leadership of Under Secretary Frank Libutti and Assistant Secretary Robert Liscouski, the IAIP Directorate leads national efforts to protect the Nation's critical infrastructures from attack or disruption. In support of this larger mission, NCSD serves as the focal point for:

? Enhancing the Nation's cyber readiness and response
? Analyzing cyber threats and vulnerabilities
? Disseminating threat warning information through alerts and warnings
? Coordinating incident response

Placement of NCSD in the IAIP Directorate ensure the integration of physical and cyber security approaches into a common, holistic risk management framework. Through the integration of physical and cyber protection capabilities, IAIP works to protect America from all threats - physical and cyber - and to understand the interdependencies that impact our critical infrastructures. Under the leadership of Assistant Secretary Liscouski, we are considering the full range of risks to the Nation, including loss of life, disruptions of infrastructure services, economic impact, and national security implications. Recognizing that future terrorist attacks may not be limited to a cyber or physical act, but rather a combination of the two to amplify impact, the Office of Infrastructure Protection is organized to examine threats and vulnerabilities across multiple dimensions:

? Integrating and mapping vulnerabilities to threats;
? Assessing sector-specific and cross-sector vulnerabilities; and
? Understanding national, regional, and local impacts.

Moreover, close linkage with the Office of Information Analysis led by Assistant Secretary Patrick Hughes, the primary threat information intelligence gathering and analysis capability of

DHS, promotes the ability to map threat information with cyber vulnerabilities. This mapping allows for the effective prioritization of potential risks so agencies may implement remediation efforts as quickly as possible to limit the impact of computer incidents.

Since June, the NCSD has worked closely with our partners in the federal government, private sector, and academia to coordinate responses to major cyber security events, such as the Blaster worm, the SoBig virus, and most recently the vulnerabilities identified in the Microsoft Windows operating system. Even though the NCSD has only been in operation for eight months, with each event, we are demonstrating our ability to quickly build capability and provide value to our stakeholders while building trust, credibility, and technical excellence that will serve as the basis for enhanced service delivery in the future.

For the remainder of my remarks, I will provide an overview of the cyber threat environment facing the Nation and the activities NCSD is undertaking with its partners to reduce our national vulnerability to these threats.

Nature of the Cyber Threat

As members of this Subcommittee have heard on numerous occasions, cyber threats continue to be a significant national and global concern. The most recent computer vulnerability identified in the Microsoft Windows operating system just two weeks ago, allowed attackers to potentially take control of a home user's computer. It is not uncommon for these types of vulnerabilities to surface in complex operating environments. The pervasive deployment of leading operating system within the United States means that vulnerabilities of this type can significantly impact the Internet and our critical infrastructures. Therefore, the US-CERT monitors these issues and generates alerts when appropriate.

When vulnerabilities are identified, viruses are launched, or when other types of cyber attacks are reported, it is often difficult to immediately identify and understand the underlying motivations for such attacks. Is it an isolated cyber attack, for example, a part of a terrorist plot, a criminal enterprise, or a teenager surfing the Net in search of a thrill? The difficulty is that the vulnerabilities and techniques that are exploited in the interest of cyber crime or even cyber hacktivisim are the same vulnerabilities and techniques that are at issue when discussing cyber terrorism.

Therefore, NCSD employs a threat-independent strategy of protecting the Internet and critical infrastructures from all types of attacks. While staying acutely aware of how terrorists might exploit the Internet, we face challenges in distinguishing between the malicious acts of a terrorist versus other types of attacks as an event is occurring in real-time. Rather than only focusing on specific attack profiles, we are developing programs and initiatives that apply to the gamut of attack approaches. In other words, our mission extends to protecting cyber systems across the entire threat spectrum, regardless of an actor's intent. If we attempt to "stovepipe" our protection efforts to focus on the different types of attackers who may use the cyber infrastructure, we risk the possibility of limiting our understanding of the entire threat environment.

While maintaining a threat-independent approach, the NCSD recognizes that DHS and the Federal government must remain vigilant in the identification of all types of cyber attackers. Components of the IAIP Directorate and our federal partners in law enforcement, defense, and intelligence devote considerable time and energy to identifying groups and individuals with the capability to launch a cyber attack and to determining the individuals responsible for an attack in the aftermath.

National Cyber Security Programs and Initiatives

As we have already discussed today, cyber attacks can appear with little or no warning, propagate quickly across cyberspace, and impact multiple infrastructures with devastating results. To lead efforts to analyze cyber threats and vulnerabilities, issue warnings, manage incidents, and coordinate response and recovery, we have established the United States Computer Emergency Readiness Team (US-CERT) to serve as the national focal point. NCSD, through US-CERT and other activities, supports three key mission areas: Analysis and Warning, Incident Management and Response, and Outreach. All of these areas support the core mission of IAIP: to make America safer through the reduction of vulnerabilities across all the critical infrastructures.

Analysis and Warning

Our top priority at NCSD is, where possible, to prevent a cyber attack from occurring and to limit its scope and impact on the critical infrastructures. A centerpiece of these efforts is the National Cyber Alert System, which is an operational system delivering to Americans timely and actionable information to secure their computer systems. Our government has a fundamental duty to warn the public of imminent threats and to provide protective measures, or at least the information necessary for the public to protect their systems. NCSD makes cyber security information products available to all computer users. These offerings alert users to security vulnerabilities, their potential impact, and actions required to mitigate the risks of exploitation. Since I was named Director of NCSD in September, we have already issued several alerts and a series of periodic "best practices" and "how-to" guidance products.

A key objective in developing the National Cyber Alert System was to provide cyber security information that is understandable to all computer users, technical and non-technical. The Internet touches all our lives, and the knowledge necessary for effective self-defense in cyberspace should be universally accessible. I am pleased to report that Americans appear to be exhibiting a keen interest in the system, which has already reached millions of citizens. On January 28, the day we inaugurated the system, the US-CERT site was bombarded by more than one million hits. Within days, more than 250,000 direct subscribers received National Cyber Alerts to maintain their cyber vigilance. For your reference and for your constituents, I would urge you to visit www.uscert.gov to subscribe to a number of our information products that facilitate the protection of your computer systems.

As referenced earlier, just two weeks ago US-CERT became aware of multiple vulnerabilities in the Microsoft Windows operating system. The most serious of these vulnerabilities allowed the potential for attackers to gain control of another user's computer through the Internet. US-CERT determined the unique nature of this particular vulnerability, when coupled with the considerable media attention surrounding its potential impact, warranted the release of a national alert. In response, US-CERT developed and released both a technical and non-technical alert distributed via the National Cyber Alert System. Importantly, the non-technical version provided easy-to-understand information to computer users about how to apply a patch in order to fix the vulnerability.

Providing timely and actionable alerts empowers home Internet users to secure their systems, and will significantly enhance our Nation's overall cyber security posture. Moreover, our alerts can enhance user response time across the public and private sectors, thereby reducing the economic impacts of virus and worm exploits. One year ago, many home users would not have heard about operating system vulnerability, like the one we learned about two weeks ago, until an attack that exploited the vulnerability made news headlines. The National Cyber Alert System reduces the warning time to minutes and hours, and we are committed to making improvements to both the warnings and the response time in the future.

In addition, thousands of additional subscribers receive our cyber alert data in a redistributed form from sources like the National Cyber Security Alliance/StaySafe Online. That alliance, whose members have committed their time and resources to regularly educating the home consumer and small businesses on good security practices, and others like it serve as a conduit to enable even greater numbers of subscribers benefiting from NCSD products. Consistent with our mission, NCSD is also partnering with the National Association of State Chief Information Officers, the Multi-State ISAC, the American Society for Industrial Security, and other security-focused groups to touch as many government agencies, private corporations and small businesses, universities, and individual citizens as possible.

Consistent with law and policy, our division also works with the Office of Management and Budget and the National Institute for Science and Technology regarding the security of Federal systems and coordinates with federal law enforcement authorities, as appropriate. To this end, we have established the Chief Information Security Officers (CISO) Forum to provide a trusted venue for the government's leading information security experts to collaborate and share experiences, capabilities, and lessons learned. NCSD also established the Government Forum of Incident Response and Security Teams (GFIRST). This activity focuses on the sharing of information on computer incidents at both the operational and technical levels. Participants represent key personnel from across the 24x7 cyber security teams servicing U.S. Government departments and agencies.

NCSD is also working with other components of DHS to capture the knowledge from field assessments with State and local governments and the private sector. Through close collaboration and integration within DHS and throughout the Federal government, the NCSD is carefully examining the cyber dependencies of key facilities and assets to determine what, if any, impact might be caused by a cyber attack. On the opposite side of the coin, NCSD is studying the potential impact of physical attacks on cyber operations.

Incident Management and Response

A pillar of the National Strategy to Secure Cyberspace was the need to create a focal point to coordinate and facilitate federal government interaction with private industry on a 24x7 basis. In response, the Department has established the US-CERT. This represents a significant accomplishment for the Department--for the first time since computer security emerged as an issue with the release of the Morris Internet worm, our national response to cyber incidents is coordinated by a single federal entity. US-CERT, in collaboration with the private sector and leading response organizations, provides a coordination center that links public and private response capabilities to facilitate communication across all infrastructure sectors. Specifically, US-CERT works on a daily basis with the Internet and computer security community and leads national efforts to analyze and reduce cyber vulnerabilities, disseminate cyber warnings, and coordinate incident response activities.

In addition to the operational partnerships that comprise the US-CERT, we have also established the Cyber Interagency Incident Management Group, or Cyber IIMG, within the federal government. The Cyber IIMG coordinates intra-governmental preparedness and operators to respond to cyber incidents and attacks. This organization brings together law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security capabilities and, importantly, possess the necessary statutory authority to act. The Cyber IIMG is developing cyber preparedness and response plans to ensure that during a cyber crisis, the full range and weight of federal capabilities are deployed in a unified and effective fashion.

To ensure the key players in the federal community can communicate during a crisis, NCSD is continuing to widen the reach of the Critical Infrastructure Warning Information Network, or CWIN. For those not familiar, CWIN is a private communications network designed to serve as a reliable and survivable network capability with no logical dependency on the Internet or the public switched network. In the event a significant cyber attack disrupts our telecommunications networks and/or the Internet, CWIN provides a secure capability for Cyber IIMG members to communicate.

I know there is great interest, particularly in the media, about how the U.S. Government might prepare for and respond to a "Digital Pearl Harbor" and an electronic September 11th scenario. The National Strategy to Secure Cyberspace stated the required technical sophistication to carry out such an attack is very high, thereby lowering its probability of occurrence. Nonetheless, it is important for us to understand and prepare for any contingency. In this vein, DHS is extending the reach of CWIN's survivable architecture beyond federal agencies by working with private sector communications backbone providers to establish CWIN nodes at their Network Operations Centers. The goal is to expand the number of CWIN nodes to 100 by the end of 2004, a significant increase, making it a robust and resilient capability that supports national cyber operations and response during times of crisis.

NCSD is actively looking for ways to test the veracity of our national response capabilities. In October 2003, we conducted Livewire, the first ever national-level cyber exercise to baseline our response capabilities to cyber attack. This exercise involved over 300 participants representing over 50 organizations across the federal, state, and local governments and the private sector. The cyber attack scenarios were developed to stress cyber interdependencies across our critical infrastructures and test our ability to collaborate across the public and private sectors. NCSD is currently working with its partners in anticipation of a follow up cyber exercise in FY05.

Outreach

An expansive and effective outreach program supports every aspect of our Division's efforts to improve and sustain cyber security. The NCSD leads and advocates the implementation of user awareness efforts; education and training programs at the K-12 and collegiate levels; and initiatives to reach out to all of our stakeholders. We realize that every link in the security chain is vital, from the Department of Homeland Security and Fortune 100 companies to the local county offices and small businesses that drive our economy. Parents and children, teachers and doctors, Internet surfers and the occasional computer user--all must be informed about the dangers of cyberspace and the need for vigilance. A key to success is aggressively pursuing an outreach agenda that recognizes a need to communicate with each of these key communities in a clear, consistent, and understandable fashion. One of our top priorities at NCSD is to communicate to the public about cyber threats and vulnerabilities in a manner that informs, reassures, and offers practical advice and solutions.

One of our most important constituencies is the private sector. Approximately eighty-five percent of America's critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003, NCSD co-hosted the National Cyber Security Summit. This event allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber

security issues facing the Nation. Based on the dialogue from that event, five industry task forces were launched, focusing in the areas of--
? Increasing awareness
? Cyber security early warning
? Best practices for information security corporate governance
? Technical standards and common criteria
? Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from national strategy development to implementation of concrete actions that both the public and private sectors could adopt to improve the security of America's cyber systems. The task forces are diligently preparing recommendations for solutions across these five key areas. The industry task forces are diligently preparing options for potential solutions in these five key areas, and NCSD stands prepared to receive and consider swift implementation of appropriate recommendations.

In addition to the National Cyber Security Summit, NCSD is working with a host of industry groups to better understand and address their issues and concerns with respect to cyber security. These groups include, amongst others, the National Infrastructure Assurance Council, the President's National Security Telecommunications Advisory Committee, and the private sector Information Sharing and Analysis Centers. We are also working closely with the research and academic communities to better educate and train future cyber analysts. These partnerships include NCSD participation in the National Science Foundation's Scholarship for Service (or "Cybercorps") program and the National Security Agency's more than 30 Information Assurance Centers for Academic Excellence.

Conclusion

At DHS the question we ask ourselves every day is "How are we making America safer today," because, in the end, this is our key metric for success. In preparing to testify today, I reflected on how far we as a country have progressed on cyber security in the past decade. The accomplishments are truly remarkable. In that time, we have created a Cabinet-level agency to bring together government, industry, and academia to manage national cyber incidents. Congress passed the Government Information Security Reform Act and the Federal Information Security Management Act, both of which have driven enhanced accountability for security of government information systems. Government agencies, private corporations, and our research community have developed, fielded, and improved security technologies, such as firewalls and intrusion detection systems, to better protect our networks. Across government, industry, and academia, organizations have created the role of a Chief Information Security Officer, or CISO, and developed computer emergency response teams to manage computer-based events. More than 30 universities and colleges are teaching information assurance courses, training our Nation's next generation of cyber defenders.

These accomplishments, when viewed in total, represent considerable progress toward making better cyber security a reality. NCSD recognizes the importance of building on these successes every day and continuing to galvanize the cyber security community, public and private. Central to our success will be furthering and reinforcing the National Cyber Security Division's reputation as a center of excellence founded on trust, credibility, and technical excellence.

Since June, I believe we have done much to further this goal. NCSD has established US-CERT, which integrated three different 24x7 federal cyber centers into one organizational entity and leveraged the vast capabilities of Carnegie Mellon's CERT/CC. We have developed a National Cyber Alert System that will reach out to all citizens and businesses, regardless of size, geography, and technical skill. We partnered with industry to create five task forces focused on key issues related to the future of cyber security. I think you will see that with each passing cyber incident, our Division will improve and refine our processes to better meet the needs of government agencies, businesses, and our citizenry.

At the same time, NCSD must continue to look forward and embark on a series of tactical and strategic cyber security initiatives designed to reduce critical infrastructure vulnerabilities. If I learned one lesson from my experiences working these issues in the private sector, it is that cyber security is an ever-moving target. Technologies, tactics, and players change quickly, and our challenge is to keep pace and to identify new areas of discovery. Software assurance, for example, represents an area of increasing importance. How do we encourage software developers to produce code with fewer embedded vulnerabilities? How do we evaluate a particular piece of code? In a world where software development is often outsourced, do we even know who wrote the source code? These types of strategic imperatives will shape the future of NCSD's programs and initiatives.

Again, I wish to thank the Chairman, the Ranking Member, and the members of the Subcommittee for this opportunity. I look forward to answering your questions.