

**Statement by
Amit Yoran
Director, National Cyber Security Division, Office of Infrastructure Protection
U.S. Department of Homeland Security
“Locking Your Cyber Front Door – The Challenges Facing Home Users and Small
Businesses”**

**Before the Subcommittee on Technology, Information Policy, Intergovernmental
Relations, and the Census
Committee on Government Reform
U.S. House of Representatives
June 16, 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 (NCSA) of the Office of Infrastructure Protection in the Department of Homeland Security's (DHS) Information Analysis and Infrastructure Protection Directorate. As we approach NCSA's one-year anniversary, I am pleased to have an opportunity to appear before the committee again to discuss the cyber security challenges facing home users and small businesses. It is important to understand the unique challenges that small businesses and home users face in their cyber security. Small businesses typically do not have the same information technology resources as large companies, and, as a result, their systems may be more vulnerable. While there is now a proliferation of computers in people's homes, many home users are not aware of cyber security threats, nor what steps they need to take to protect themselves. To help all of these groups increase their cyber security, we have established a series of programs geared towards home users and small businesses that focus specifically on their needs and level of understand. Thus, the outreach, awareness, and education initiatives by NCSA provide crucial information and resources to help secure the computers of home users and small businesses.

Introduction

NCSA was created in June 2003 to serve as the 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 and initiatives. 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, education and awareness, 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

Tools and Strategies Available to Home Users and Small Businesses

A core component of Priority III of the Strategy is to promote a comprehensive national awareness program to empower all Americans, business, the general workforce, and the general population, to secure their portion of cyberspace. The Strategy clearly identifies home users, small and large enterprises, institutes of higher education, the private sectors that own and operate the vast majority of the Nation’s cyberspace, and state and local governments as the users and cyber security stakeholders. We are reaching out to, and partnering with, each of these groups in addition to other groups within the Federal Government.

DHS recognized that in order to meet many of the mandates in the Strategy and other objectives addressing greater national cyber security, we needed to create an operational mechanism for building a cyber security readiness and response system. As such, through a partnership with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, we created the U.S. Computer Emergency Readiness Team, or US-CERT. Through the partnership, US-CERT is able to leverage, rather than duplicate, existing capabilities and accelerate national cyber security efforts. US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation’s cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States, as well as the cyber consequences of physical attacks. To this end, US-CERT has built a cyber watch and warning capability and is launching the US-CERT Partner Program to build situational awareness, cooperation, and coordination with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber – and physical – attacks. Through the Homeland Security Information Network (HSIN)/US-CERT secure portal, US-CERT is a crucial component of – and a distribution tool for – cyber security awareness activities.

DHS and the US-CERT are engaged in several activities that enhance our communication to the public in a variety of ways. I will outline them in my testimony today, but first I want to share with you our newest initiative. I am happy to announce that US-CERT and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are forming a joint partnership focused on developing a series of national webcasts which will examine critical and timely cyber security issues. The first webcast to be launched in this series will be open to government participants and will take place next Tuesday, June 22nd. Embracing the concept that *security is everyone's responsibility*, these webcasts will be archived, put on the website, and will be open to public view to help raise awareness and knowledge levels. The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. Webcast sessions will feature variety of cyber security topics that are both technical and non-technical, and future sessions may focus specifically on home users and small businesses. There is no charge for participation in the webcasts, which makes them accessible to home users and small businesses. DHS views these webcasts as another strategic awareness tool that will further help home users and small businesses improve their cyber security posture.

On January 28, 2004, the Department of Homeland Security, through US-CERT, unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely and actionable information to Americans to secure their computer systems. As the U.S. Government, we have a fundamental duty to warn the public of imminent threats and to provide protective measures when we can. It is our responsibility to provide actionable information to the public so that they can take the necessary precautions to protect their systems. Furthermore, it is also important to inform the public about the true nature of a given incident, what the facts and possibilities are, and, most importantly, what the potential consequences may be if preventative action is not taken. This information is especially crucial in helping home users and small businesses secure their systems. The offerings of the National Cyber Alert System provide detailed and accurate information about imminent threats and incidents. We have already issued several alerts and the initial products in a periodic series of "best practices" and "how-to" guidance messages. To help educate home users and small businesses, regardless of computer skill-level, the alert system provides information in both technical and non-technical format. Additionally, US-CERT cyber tips help to educate home users on basic security practices and increase overall awareness. Since the release of the system, DHS has issued alerts on such topics as: "Understanding Firewalls;" "Good Security Habits;" "Choosing and Protecting Passwords;" and "Why is Cyber Security a Problem?"

I am pleased to report that Americans are exhibiting a keen interest in the alert system. On day one of the National Cyber Alert System launch we had more than one million hits to the US-CERT website. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. As we increase our outreach, the National Cyber Alert System is investigating other vehicles to distribute information to as many Americans as possible.

DHS is aware of the power of the media as an education and awareness vehicle, as well as a significant form of outreach to home users and small businesses. We launched an outreach program concurrent with the launch of the National Cyber Alert System. In nine days, we generated almost one thousand media placements across national newspapers, trade publications, web sites, as well as television and radio broadcast media. Feature coverage on CNN, Fox News, NBC News, National Public Radio, and in *The Wall Street Journal*, *The Washington Post*, *Newsweek*, and *The New York Times* generated millions of impressions, increasing American's cyber security awareness and driving citizens to visit the US-CERT website to subscribe to the National Cyber Alert System.

An industry-led coalition of interested security experts from the public and private sector was created as part of the National Cyber Security Summit process in December of 2003. At that time, the Awareness and Outreach Task Force was established to provide recommendations for increasing awareness among home users and small businesses. In March, 2004, this task force submitted its recommendations to the National Cyber Security Partnership. A number of these recommendations are being considered by DHS as a part of both an overall awareness effort and the partnership between DHS and the National Cyber Security Alliance and other groups.

DHS is also a sponsor of the National Cyber Security Alliance (NCSA) and *StaySafeOnline*, a public-private organization created to educate home users and small businesses on cyber security best practices. Other NCSA sponsors include: The Federal Trade Commission, AT&T, America Online, Computer Associates, Information Technology Association of America, Network Associates, and Symantec. DHS is providing matching funds to expand the NCSA end-user outreach campaign, which will include a Fall 2004 Public Service Announcement to increase awareness among Americans about key cyber security issues. We look forward to working actively with the NCSA to increase the profile and impact of its semi-annual National Cyber Security Day initiative. Coinciding with the days that we reset our clocks in the spring and fall, the National Cyber Security Day program encourages Americans to review and improve their cyber readiness. We will utilize the National Cyber Security Days as a focal point to heighten our awareness efforts. In addition, we are working with NCSA on a series of other educational and awareness programs, including collaborative initiatives with Internet Service Providers and developing cyber security educational tool kits. We will be pleased to make these resources available to you for use in your districts.

NCSD is also partnering with the Department of Justice's Bureau of Justice Statistics (DOJ/BJS) to study the effects of cyber crime in the U.S, including crimes affecting home users and small businesses. Although a number of other studies related to cyber crime are conducted every year, none of these studies has ever been statistically valid, due to their scope, format, question samples, or response rate. NCSD was approached earlier this year by the DOJ/BJS to partner in this significant effort to undertake the first widespread and statistically valid study of cyber crime. The initial distribution will be to 36,000 thousand individuals and businesses, including small businesses, covering all of the critical infrastructure sectors and the goal survey response

rate is 60 percent. By comparison, the most widely referenced, current, annual survey on cyber crime is distributed to less than 2000 businesses, and has never received a response rate of better than 15 percent. The goal of the survey is to provide comprehensive and statistically relevant information on the subject of cyber crime in the United States for the first time. This information can be used by industry in any number of ways, including strategic information technology security planning and resource allocation, and can help better prepare small businesses target specific, cyber security needs.

Finally, the U.S. Government is pursuing a number of avenues to address cyber security in our education system and working closely with the research and academic communities to better educate and train future cyber analysts. Recent successes include a Memorandum of Agreement (MOA) between DHS and the National Security Agency (NSA) to expand NSA's Centers of Excellence in Information Assurance Program into a national program. This will accelerate and expand the current program, attain national prominence, and result in participation from additional universities. The net result is that the U.S. will be furnished with a growing number of cyber security professionals. Government at all levels, corporations, small businesses, and the general public all benefit from educating a strong force of highly educated information assurance professionals.

Conclusion

DHS is committed to providing effective cyber security tools and education to home users and small businesses through our many outreach, awareness, and education efforts. The establishment of the US-CERT and its National Cyber Alert System provide the first step toward a national awareness campaign. As previously described, the alert system provides periodic alerts, tips, best practices and other guidance for dissemination to all sectors of our society. DHS also provides cyber security tips to home users and small businesses through the National Cyber Security Alliance *StaySafeOnline* campaign to help educate all users about basic security practices and to increase overall awareness as well as cyber security tool kits that can be disseminated to both groups.

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