Statement for the Record

Jerry Dixon
Director, National Cyber Security Division
U.S. Department of Homeland Security

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on
Emerging Threats, Cybersecurity and Science and Technology

April 19, 2007

Chairman Langevin**,** Ranking Member McCaul and Members of the Subcommittee, I appreciate the opportunity to address you on the National Cyber Security Division's (NCSD) role in detection of and response to intrusions of Federal computer networks. The NCSD is a component of the Office of Cyber Security and Communications (CS&C) within the recently established National Protection and Programs Directorate (NPPD) of the Department of Homeland Security. Assistant Secretary for Cyber Security and Communications Gregory Garcia is responsible for the overarching mission of CS&C to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's IT and communications infrastructure. This mission is part of a larger strategy to ensure the security, integrity, reliability, and availability of our information and communications networks. Indeed, the very topic of this hearing – that is, the need to coordinate better cyber security practices across the Federal government – is among Secretary Chertoff's highest priorities.

The NCSD was created in June 2003 to serve as a national focal point for cyber security and to coordinate implementation of the *National Strategy to Secure Cyberspace* ("the *Strategy*") issued by President Bush in February 2003. The *Strategy* outlines a national framework of priorities, which are reflected in NCSD programs, to promote cyber security and public-private partnerships. The NCSD's mandate includes analysis, watch and warning, information sharing, vulnerability reduction, aiding national recovery efforts for critical infrastructure information systems, and working collaboratively with the public and private sectors to secure America's cyber networks, systems, and assets. DHS works across its component entities to address cyber security in a cohesive manner, as well as with our Federal partners across the departments and agencies.

The NCSD's watch and warning mechanism for cyber infrastructure is the United States-Computer Emergency Readiness Team (US-CERT). This team provides around-the-clock monitoring of cyber infrastructure and coordinates the dissemination of information to key constituencies including all levels of government and industry. DHS and

NCSD/US-CERT serve as the focal point for helping government, industry, and the public work together to achieve the appropriate responses to cyber threats and vulnerabilities

A key area of focus for NCSD/US-CERT is our work with the Federal departments and agencies.

Programs and Initiatives

The NCSD/US-CERT has a number of programs and initiatives to accomplish our operational mission of coordinating improvements in the security and management of the Federal Government's information systems and networks. These programs focus on enhancing situational awareness, increasing collaboration across Federal operational security teams, preventing or quickly containing cyber incidents, and providing for inter-agency coordination during a cyber event.

The NCSD manages the Einstein program, which supports Federal agencies' efforts to protect their computer networks. Einstein provides the first situational awareness picture of the Federal Government's Internet facing networks. It enables the rapid detection of cyber attacks affecting agencies and provides Federal agencies with early incident detection. Einstein is currently deployed at ten Federal agencies with a goal to deploy it to all Cabinet level and critical independent Federal agencies.

Einstein has greatly reduced the time for the Federal Government to gather and share critical data on computer security risks from days to hours.

Another major program is the Information Systems Security Line of Business (ISS LOB). The NCSD was designated by OMB as the managing agency for the ISS LOB, which is part of the President's Management Agenda. The ISS LOB allows all Federal departments and agencies to benefit from improved levels of cyber security, reduced costs, elimination of duplicative efforts, and improved quality of service and expertise. The program addresses four information security areas that are common across the Federal Government: Security Training, Federal Information Security Management Act (FISMA) Reporting, Emerging Security Solutions for the Lifecycle, and Situational Awareness and Incident Response.

Additionally, CS&C's mission is enhanced through the continued development of the National Response Plan (NRP). The NRP provides the structure and mechanisms for Federal support to State, local, and tribal incident managers. In coordination with other Federal agencies, CS&C has been working to provide mechanisms for improving national-level response to Information Technology and Communications incidents. The Cyber Incident Annex to the NRP provides a framework for addressing a cyber event which requires a federally coordinated response, and it formalizes the National Cyber Response Coordination Group (NCRCG) as the principal Federal interagency mechanism to coordinate preparation for and response to a national-level cyber incident. The NCRCG, co-chaired by DHS, Department of Defense, and Department of Justice, coordinates recommendations and facilitates direct actions to obtain the necessary interagency support to respond to major cyber incidents.

Through the NCSD exercise program, we regularly test our plans and procedures. In February 2006 we held the first national cyber exercise, "Cyber Storm," to examine various aspects of our operational mission. This included the activation of the NCRCG and working with other Federal agencies on cyber security response to address the exercise scenarios. Lessons learned and after action items from that effort continue to be addressed by NCSD and other participants. Progress made to improve response processes and procedures since Cyber Storm, as well as other regional exercises that we sponsor, will be measured in Cyber Storm II, which is scheduled for March 2008.

We also worked collaboratively with the Air Force, the National Institute of Standards and Technology (NIST), the Defense Information Systems Agency, the National Security Agency, and Microsoft to establish common security configurations for Windows XP and VISTA. Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information. The configurations can be found on our website and we are working with NIST to help agencies adopt them.

Finally, the US-CERT Operations Incident Handling Center provides a 24 hour a day, seven day a week watch center that conducts daily analysis and situational monitoring. The Center identifies trends and provides information on incidents and other events, as they are detected and unfold, to increase situational awareness and understanding of the current operating environment. FISMA policy requires all Federal agencies to notify US-CERT of any data breaches, unauthorized access, or suspicious activity, including the loss of personally identifiable information (PII).

Recent Response Efforts

The NCSD/US-CERT played a pivotal role in response efforts to the recent incidents at the Department of Commerce (DOC) and the Department of State (DOS). Both incidents highlight that the threat to government systems has shifted from opportunistic hacking to targeted cyber attacks. These cyber attacks are sophisticated and have often led to the discovery of new vulnerabilities in applications or operating systems. As a result of these vulnerabilities, NCSD/US-CERT works closely with those vendors whose products are affected to collaborate on fixes and mitigation strategies, which are communicated to our partners within government and industry via the National Cyber Alert System. These incidents highlight the need for enhanced rapid situational awareness across the Federal Government. In addition, the Einstein early watch and warning system has been implemented at the DOS and groundwork is being laid to implement Einstein at the DOC in the near future.

In both incidents, the affected Departments notified the US-CERT in compliance with OMB guidance, FISMA, and the US-CERT Concept of Operations (CONOPS) within the required timeframes. While the details of these incidents should be provided by DOS and DOC, I will discuss the effective coordination processes that were utilized to respond to these incidents. We would be happy to provide the Committee with a more detailed briefing in the appropriate setting at a later date.

In the DOS incident, which involved a newly identified Microsoft "zero-day" vulnerability, the US-CERT immediately engaged to assist with response efforts as soon as the report was received. In collaboration, the DOS and US-CERT coordinated with the National Operations Center (NOC), and other Federal agencies throughout the incident response and recovery phase. At the same time, US-CERT coordinated daily with the Microsoft Security Response Center for vulnerability management, patch remediation and public disclosure coordination.

Additional technical analysis revealed this vulnerability to be more dangerous and pervasive across all Microsoft operating system platforms. Just prior to the public release of the Microsoft Security Bulletin (MS06-040), the US-CERT and Microsoft conducted a series of briefings with Federal and State operational Incident Response and Security Teams, Chief Information Officers, Chief Information Security Officers, and critical infrastructure sectors via the Sector Coordinating Committees (SCC) and designated Information Sharing and Analysis Centers (ISAC).

Following these briefings, the US-CERT and Microsoft jointly released public notifications related to the new vulnerability and the availability of a security patch. The US-CERT released a public Technical Cyber Security Alert via the National Cyber Alert System. Additionally, we disseminated a Federal Information Notice to the Federal community, and a Critical Infrastructure Information Notice to the critical infrastructure SCCs and ISACs.

Because of the significant risk posed by this vulnerability, DHS released its first ever press release focused on cyber security recommending that all users of the Microsoft Windows Operating Systems apply the security patch as quickly as possible. This public press release, along with the significant volume of media coverage and attention it garnered, led to a highly successful rollout of a security patch. Also the US-CERT continued to monitor the Federal Government's patch status and reported those results on a weekly basis until all agencies reported they had completed their patch deployments.

In the incident involving the DOC, the US-CERT was notified by the DOC's Office of the Chief Information Officer and Cyber Incident Response Team (CIRT) in accordance with OMB guidance, FISMA, and the US-CERT CONOPS. During this response effort, the US-CERT provided on-site assistance at the request of DOC CIRT. This enabled on-site collaboration and rapid analysis of the event so it could be quickly contained and remediated. In addition, they coordinated their activities with the NOC and other Federal agencies throughout the incident response and recovery phase. As a result of this incident the DOC has expanded their response capability to an around-the-clock operation which should greatly aid in their future incident detection and response efforts.

The NCSD continues to conduct outreach to Federal agencies to raise cyber security awareness with operational security teams and senior officials through its Government Forum of Incident Response and Security Teams (GFIRST). Moreover, the NCSD continues to work with our Federal and private sector stakeholders to identify vulnerabilities and quickly identify suspicious activity by enhancing bi-directional information sharing. The NCSD also continues to provide cyber security training to further increase the number of cyber incident responders to enable agencies to quickly identify and contain emerging cyber attacks.

While significant progress has been made to enhance the network security of Federal departments and agencies, more can and will be done. Based on our ongoing programs and initiatives, the NCSD and its US-CERT are poised to continue to work towards achieving greater overall cyber security with our Federal, State, local, tribal, international, and private sector partners. It is clear from our work to date and the continuing evolution of information technology in our society that additional advancements will be required to mitigate the growing cyber security risks. Accordingly, we expect continuing dialogue with this Committee as we further understand the evolving nature of the cyber security issues.

Thank you for the opportunity to appear before this Subcommittee today and I would be happy to answer any questions you may have at this time.