Statement for the Record
Robert D. Jamison
Under Secretary for National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
February 28, 2008

Introduction

Chairman Thompson, Congressman King, and Members of the Committee, I appreciate the opportunity to speak about the Department of Homeland Security's ongoing efforts to improve cybersecurity. I also appreciate the Committee's continued interest in the Department's cybersecurity activities and in particular the Department's role in Comprehensive National Cybersecurity Initiative. As we have done since last year, the Department and our interagency partners will continue to engage with the Committee and Congress in an appropriate setting on the classified portions of our activities.

As our economy, critical infrastructure, and national security become more reliant on technology, it is essential that we take proactive measures to enhance the security and resiliency of the information technology (IT) systems and networks on which we rely. We face increasing global threats to our cyber infrastructure, and the exploitation of vulnerabilities is facilitated by the widespread availability of tools, techniques, and information. The Department has made progress in enhancing the cybersecurity of the Nation; however, we recognize the need to take deliberate action to reinforce and build on those efforts as the threat grows. To underscore the Department's efforts in this area, Secretary Chertoff has identified cybersecurity as one of the top priorities for the Department for 2008. The enacted fiscal year 2008 and the President's proposed fiscal year 2009 budget reflect the necessary investment for this priority.

The Department has outlined four areas of focus within cybersecurity to guide our efforts over the coming year. First, we are enhancing Federal cyber situational awareness, intrusion detection, information sharing, and response capabilities. Second, we are expanding the Department's cadre of cybersecurity personnel, its capabilities, and its services to our public and private sector partners. Third, we are strengthening our efforts to integrate cybersecurity into Federal, State, private sector, and international preparedness, response, and resilience efforts. Finally, we are developing and promoting the adoption of proven cybersecurity practices with government, private sector, the general public, and the international community.

Today, I will provide an overview of the Department's efforts to improve cybersecurity across Federal departments and agencies will focus on our first priority. Specifically, I will address two programs focused on cyber risk reduction across the Federal enterprise: the Trusted Internet Connections initiative (TIC) and the EINSTEIN program.

Cybersecurity: A Departmental Priority

As Under Secretary for the National Protection and Programs Directorate (NPPD), I oversee the Directorate's efforts to advance the Department's mission of risk reduction, which encompasses identifying threats, determining vulnerabilities, and targeting resources where risk is greatest, including to our critical information systems. A key area within this mission includes the Office of Cybersecurity and Communications' (CS&C) efforts to improve cybersecurity by reducing risk to the Nation's cyber infrastructure and maintaining the resilience of our communications systems. The 2007 *National Strategy for Homeland Security* articulated the importance of this mission by recognizing that many of our essential and emergency services, including our critical infrastructure, "rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent [Critical Infrastructure and Key Resources] and ultimately to our economy and national security."

Global threats to our cyber infrastructure and to the services, systems, and assets that depend on them continue to increase. The nature of the threat is large and diverse and ranges from unsophisticated hackers to very sophisticated adversaries. We are seeing more state-of-the-art intrusion techniques designed to disrupt, deny access to, degrade, or destroy critical information systems and steal our intellectual capital and proprietary information.

The Department is positioned to address these threats through our watch, warning, and response capabilities; our information sharing and coordination efforts with the public and private sectors; and our programs and initiatives through the National Cyber Security Division (NCSD) and United States Computer Emergency Readiness Team (US-CERT). These programs and initiatives are designed to carry out our mission of preparing for and responding to incidents that could degrade or overwhelm the operation of our Federal IT and communications infrastructure.

Securing Federal Departments and Agencies

Since its inception, the Department of Homeland Security has been working to strengthen Federal and critical infrastructure systems and enhance our cyber operational response capabilities. The Department established a number of programs and initiatives to coordinate efforts with Federal departments and agencies to improve cybersecurity. These programs focus on enhancing situational awareness, increasing collaboration across Federal operational security teams, preventing cyber incidents, and providing inter-agency coordination during a cyber event.

The Department conducts outreach to Federal departments and agencies to raise cybersecurity awareness with operational security teams and senior official through channels such as the Government Forum of Incident Response and Security Teams (GFIRST). GFIRST is a community of more than 50 incident response teams from various Federal agencies working together to improve Federal Government security. The Department sponsors the annual GFIRST Conference, which fosters greater information sharing among IT security professionals from various departments and agencies. The 2007 conference garnered unprecedented attendance, including more than 550 IT professionals, representing numerous Federal departments and agencies, including more than 100 attorneys from the Department of Justice. We expect similar success at the upcoming GFIRST Conference in June 2008.

To enhance collaboration on control systems security across the Federal Government, NCSD established and facilitates the Federal Control Systems Security Working Group, consisting of over 30 government organizations. Since late 2006, this group has been developing a Federal Coordinating Strategy to Secure Control Systems, which seeks to place related Federal control systems activities into a unified framework, assess opportunities for sharing and leveraging information and resources, and identify possible gaps in Federal efforts. In addition, NCSD is working with other Federal organizations, such as the Tennessee Valley Authority and the U.S. Army Corps of Engineers, to provide control systems specific tools in their areas of responsibility.

NCSD co-chairs the National Cyber Response Coordination Group (NCRCG) with the Department of Justice (DOJ) and the Department of Defense (DoD) to coordinate response to a cyber incident across the Federal Government. The NCRCG serves as the principal interagency mechanism for providing subject matter expertise, recommendations, and strategic policy support to the Secretary of Homeland Security during and in anticipation of a cyber incident. The NCRCG comprises senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents. The senior-level membership of the NCRCG helps ensure that during a significant national incident, appropriate Federal capabilities will be deployed in a coordinated and effective fashion.

To ensure processes and procedures involved with response to cyber incidents are up to date and comprehensive, the Department sponsors exercises to allow participants in the public and private sector to examine their cyber response capabilities. In February 2006, the Department held the first National Cyber Exercise – Cyber Storm – to examine various aspects of our operational mission, including collaboration with Federal departments and agencies. The Department and other participants continues to address lessons learned and after action items from the exercise. Progress made to improve response processes and procedures will be measured in Cyber Storm II, which is scheduled for March 2008. Cyber Storm II will simulate a coordinated, large-scale cyber attack on four of the Nation's critical infrastructure sectors. The exercise will include participants from 18 Federal departments and agencies, nine States, over 40 private sector companies, and four international partners. For the Federal Government Cyber Storm II will exercise strategic incident response decision-making and interagency coordination in accordance with national-level policies and procedures. The exercise will strengthen the ability of participating organizations to prepare for, protect against, and respond to the effects of cyber attacks.

US-CERT is the Department's watch and warning mechanism for the Federal Government's Internet infrastructure. It provides around-the-clock monitoring of Federal network infrastructure and coordinates the dissemination of information to key constituencies including all levels of government and industry. In addition, US-CERT serves as the main component for helping government, industry, and the public work together to respond to cyber threats and vulnerabilities. A main area of focus for US-CERT is our work with Federal departments and agencies. US-CERT provides government partners with actionable information needed to protect information systems and infrastructures. In addition, US-CERT leverages its technical

expertise to further efforts to secure Federal networks and systems through targeted programs, such as the Trusted Internet Connections (TIC) initiative and EINSTEIN.

Trusted Internet Connections Initiative

The Trusted Internet Connections (TIC) initiative is a multifaceted plan to improve the Federal Government's security posture by significantly reducing the number of Federal external connections. External connections include, but are not limited to, any connection outside a department or agency, such as government-to-government connections and Internet access points. Currently, there are several thousand Federal external connections. The existence of such a large number inhibits the Federal Government's ability to implement standardized security measures effectively. The TIC initiative aims to reduce and consolidate the number of external connections to create a more clearly defined "cyber border." Fewer external connections will enable more efficient management and implementation of security measures and reduce avenues for malicious attacks. Once fully implemented, the TIC initiative will facilitate security standardization for access points across the Federal Government.

The Office of Management and Budget (OMB) maintains oversight of the TIC initiative, and implementation relies on the technical expertise of US-CERT, all participating Federal departments and agencies, and the Information Systems Security Line of Business (ISS LOB). The ISS LOB is part of the President's Management Agenda to expand Electronic Government. The goal of the ISS LOB is to address those areas of information security which are common to all agencies and are not specific to the mission of any individual agency, ultimately resulting in improved information systems security. OMB has selected DHS as the managing agency for the ISS LOB, and DHS, through the NCSD, is leveraging its role in the ISS LOB to enhance the TIC initiative.

OMB announced[1] the TIC initiative to the heads of Federal Government departments and agencies in November 2007, subsequently outlining the specific steps departments and agencies should take as part of the initiative, including compiling a comprehensive inventory of each department and agencies' existing network infrastructure. Each department and agency is required to develop a Plan of Actions and Milestones (POA&M) to reduce and consolidate the number of external connections with a target completion date of June 2008. NCSD is in the process of reviewing initial POA&M submitted to NCSD, via the ISS LOB, for review to ensure completeness and alignment with the goals and objectives of the TIC initiative. In addition, US-CERT and the ISS LOB created an interagency technical working group to establish, for OMB's approval, a list of requirements and standards for the implementation of each TIC. Once approved, these requirements will be passed to the department and as for implementation.

The reduction of external connections will have a number of benefits for the Federal Government, particularly when coupled with other security measures. First, fewer external connections will provide the ability to establish a central oversight and compliance function. This central function will benefit Federal systems by facilitating the implementation of standardized information security policies. In addition, the TIC will enable the implementation of 24-hour watch and warning capabilities across the Federal Government and enable faster and more effective response to cyber incidents. The TIC will also enable the rollout of an intrusion

[1] The TIC was announced in OMB Memorandum 08-05.

detection system across Federal networks to provide better situational awareness, earlier identification of malicious activity, and overall, a more comprehensive network defense.

The EINSTEIN Program

The EINSTEIN program is another critical element of our efforts to increase cybersecurity across Federal departments and agencies. EINSTEIN is a collaborative information-sharing program that was developed in response to increasingly common network attacks on and disruptions to Federal systems. The program was initially established to help departments and agencies more effectively protect their systems and networks and to generate and report necessary IT-related information to US-CERT. EINSTEIN enhances situational awareness of the Federal Government's portion of cyberspace, allowing US-CERT and cybersecurity personnel to identify anomalies and respond to potential problems quickly. EINSTEIN is presently deployed at 15 Federal agencies, including the Department of Homeland Security, and US-CERT is in the process of deploying EINSTEIN across all Federal departments and agencies. With the TIC initiative providing a reduced number of external connections, EINSTEIN will be able to more effectively monitor activity across Federal Government networks.

The EINSTEIN program supplements departments' and agencies' intrusion detection systems by monitoring their networks from outside their firewalls, 24 hours a day, seven days a week. EINSTEIN utilizes an automated process for rapidly collecting, correlating, analyzing, and sharing government computer security information with US-CERT and department and agency system administrators. EINSTEIN utilizes a specific tool set to analyze network flow, which is comprised of a brief summary of a network connection, including source, destination, time, bytes, and packets transferred.

US-CERT deploys EINSTEIN to Federal departments and agencies, along with all necessary hardware, software, support services, and staff training. Once implemented within a Federal department or agency, EINSTEIN identifies and establishes a baseline for normal network operational activity. From this baseline, security personnel are able to identify unusual network traffic patterns and trends, such as configuration problems, unauthorized network traffic, network backdoors, routing anomalies, and unusual network scanning activities. With this information, security personnel can quickly identify, prevent, and respond to potential problems.

EINSTEIN analyzes the information collected and posts it to a secure Internet portal, which only approved personnel can access. System administrators from participating departments and agencies review their data and determine if any mitigation activities are necessary, often in collaboration with US-CERT. Simultaneously, US-CERT personnel analyze the data from participating department and agency networks to determine if any recurring patterns and trends exist, potentially indicating the presence of malicious cyber activity targeting the Government as a whole. If US-CERT finds such patterns of unusual activity across multiple agencies, US-CERT notifies appropriate stakeholders and coordinates mitigation and response actions as necessary.

EINSTEIN already has proven successful in enhancing security within the Federal Government. For example, through the Department of Transportation's (DOT's) participation in the EINSTEIN program, we were able to quickly detect malicious activity and prevent it from

infecting other government computers. In this case, a computer worm had infected an unsecured government computer in a U.S. Government agency. When the worm, in its attempts to increase its network of infected computers, tried to attack DOT's network, EINSTEIN detected the unusual traffic. After further investigation, US-CERT discovered the worm and worked with the affected departments and agencies to prevent its spread.

EINSTEIN reduces the time it takes to gather and share critical data on computer security risks from an average of four to five days to an average of four to five hours. Quick notification results in the Federal Government being able to respond to incidents and mitigate potential problems more efficiently and effectively. Government-wide deployment of EINSTEIN will further enhance the ability of US-CERT to gain a more comprehensive view of Federal systems, increasing US-CERT's analytic capabilities and augmenting the extent and quality of US-CERT's information sharing activities. Together with the TIC, broad deployment of EINSTEIN will increase our ability to address potential threats in an expedited and efficient manner.

Conclusion

Securing the Nation's IT systems and networks in an environment of increasing global threats by agile and sophisticated adversaries is a difficult challenge that requires a coordinated and focused effort. Secretary Chertoff's prioritization of cybersecurity for the year ahead underscores the importance of this challenge. Accordingly, the Department is working with its Federal partners to develop and implement a holistic strategy for securing our Federal networks and systems.

We have established a strong foundation of programs and activities to address the dynamic threat, and we continue to expand and improve upon those programs through new and enhanced efforts. The TIC's reduction of Internet access points and EINSTEIN's situational awareness capabilities are examples of initiatives designed to prevent the disruption of Federal critical infrastructure from unauthorized users that penetrate Federal systems and steal or compromise vital or sensitive information.

Government-wide deployment of TIC and EINSTEIN enables strategic, cross-agency assessments of irregular or abnormal Internet activity that could indicate a vulnerability or problem in the system. These programs enhance Federal Government cybersecurity by providing more robust security monitoring capabilities to facilitate the identification and response to cyber threats and attacks. They contribute to the improvement of network security, increasing the resilience of critical electronically delivered government services, and enhancing the survivability of the Internet.

The Federal Government is committed to increasing its capabilities to address cyber risks associated with our critical networks and systems. Every Federal department and agency plays a role in and adds to the protection of our Nation and its citizens from cyber threats.

Thank you for your time today, and I am happy to answer any questions from the Committee.