

**Statement for the Record
Dr. Peter Fonash
Acting Director, National Cybersecurity Division
Chief Technology Officer, Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security**

**Before the
United States House of Representatives
Committee on Science and Technology
Subcommittee on Technology and Innovation
Subcommittee on Research and Science Education
June 16, 2009**

Introduction

Good afternoon, Chairman Wu, Chairman Lipinski and Members of the Subcommittees. Thank you for the opportunity to speak about the Department of Homeland Security's (DHS) ongoing efforts to secure the Federal Executive Branch civilian networks and information systems, the White House's recently released Cyberspace Policy Review, as well as coordinating activities focused on securing portions of the Nation's critical infrastructure.

One of the greatest threats facing our Nation is a cyber attack to our critical infrastructure and key resources (CIKR), on which our Nation depends. Our information communications technology systems are integral to our daily lives. Our society relies on technology and telecommunications to support our economy and business operations, and also support critical functions of Government. An attack could cause disruption to any or all of our key sectors and could jeopardize not only the private sector, but the Government's ability to provide critical services to the public. Such an attack could also create cascading effects throughout the country due to the integrated and global nature of business today.

The cyber threats to these systems are very real, growing, and evolving. The Nation must be vigilant, proactive, and innovative in its efforts to address and mitigate disruptions of service. What makes this endeavor ever more challenging is the volume and composition of these threats. They are large and diverse and range from independent unsophisticated opportunistic hackers to very technically competent adversaries and nation states.

Our adversaries—both criminal and nation states—have become increasingly sophisticated in their methods and ability to coordinate malicious activities. The United States Government is aware of, and has responded to, malicious cyber activity directed at its civilian and military systems and networks over the past few years. We continue to remain concerned that this activity is growing more sophisticated, more targeted, and more prevalent.

I am here to underscore the Department's resolve to collaborate and share actionable information with stakeholders to mitigate known threats. Engagement, however, cannot be a one-way information flow with the goal of simply relaying information. We must create a 2-way dialogue and facilitate continuous feedback that helps us improve notification products, such as informational notices and situational awareness reports.

Information sharing is an essential part of cybersecurity and we must continue to increase our current public/private information sharing and coordination efforts via the National Infrastructure Protection Plan (NIPP) framework. Using the NIPP framework, DHS has built robust working channels to exchange and integrate information with and among our partners in industry. Our efforts in this area have already begun. Through the Cross-Sector Cyber Security Working Group (CSCSWG), we have convened an Information Sharing Subgroup to look at ways to facilitate the bi-directional sharing of cyber information, indications, and warnings through the operational capabilities within and across the sectors and government. Specifically, we are looking at how to better share cyber threat and vulnerability information with those in industry who need it, understanding that some of this information is very sensitive. We are also developing plans on how to work with industry partners to obtain greater situational awareness on the status of CIKR networks.

As you know, DHS is the lead agency in a multi-agency approach in coordinating the security of Federal Executive Branch civilian networks. In large part, activities currently under way are due to the creation of the Comprehensive National Cybersecurity Initiative (CNCI), which is designed to further protect Federal networks and explore new ways to assist industries in securing their infrastructure. There is wide agreement that the CNCI moved the ball in the right direction. However, more needs to be done. President Obama's call for, and subsequent completion of, the White House Cyberspace Policy Review reaffirms that cybersecurity and cyber threats are among the most significant issues facing the economic and national security of our Nation.

At DHS we have been focused on three main areas as part of the CNCI:

- 1) Establishing a front line of defense;
- 2) Seeking ways to defend against a full spectrum of threats through intelligence and supply chain security; and
- 3) Taking cybersecurity to the next level through workforce education.

Over the last year, DHS has been leading the effort to establish a front line of defense by reducing vulnerabilities and preventing network intrusions in the Federal Executive Branch civilian networks. We are improving our cybersecurity posture in this area by focusing government efforts on reducing external connections through the Trusted Internet Connection program and deploying EINSTEIN, our intrusion detection system. DHS is also working in close coordination with our interagency partners to develop additional capabilities and capacity to detect and eventually prevent intrusions. Such collaboration with our Federal partners will also help to inform the products necessary to provide actionable information to our CIKR community.

The Department is also seeking ways to better protect Federal Executive Branch civilian information systems and networks from the full spectrum of threats, such as from malicious code embedded in hardware or software products. This requires improving our global supply chain defense through increased awareness of threats, vulnerabilities, and consequences as well as collaborating with the National Institute of Standards and Technology in the development of standards, policies and best practices across the Federal civilian enterprise. In conjunction with the Department of Defense (DoD), DHS is working to increase the capabilities of all federal departments and agencies to ensure the protection of their supply chains as well as their ability to mitigate risks.

A strong workforce is also necessary to ensure the continual advancement of our cybersecurity posture. Successful detection and mitigation of threats requires us to maintain a workforce at a high skill level. For the safety of our information systems and networks, now and in the future, DHS is focusing its resources on building the next generation cyber workforce by improving workforce training and education, recruiting new talent, and providing funding for college and university scholarships.

In addition, we are working with industry and Government partners to secure the Nation's critical infrastructure networks. As you well know, the Federal Government does not own the Nation's information technology networks or communication infrastructures. The vast majority of the Nation's cyber infrastructure is in the hands of the private sector. For this reason, cybersecurity is not exclusively a Federal responsibility, and as I mentioned earlier, collaboration with the private sector is essential.

The Department's National Cyber Security Division (NCSD) serves as the national focal point for cybersecurity on behalf of the Department. The NCSD works in concert with the DHS Science and Technology Directorate to cohesively develop technologies that address current and future technology gaps. The NCSD also works with the private sector and Federal, State, local, tribal and international governments to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. The Department maintains a strong and positive relationship with the National Security Agency (NSA). NSA has provided a number of senior level detailees to the Office of Cybersecurity and Communication (CS&C) and the National Cyber Security Division (NCSD) within CS&C. These personnel assist in the execution of CNCI and provide integral technical and operational expertise to the Department as we build our capacity and capabilities. It is a true team effort. More broadly, NCSD through United States Computer Emergency Readiness Team (US-CERT) coordinates and shares incident information with law enforcement, the intelligence community, as well as other key stakeholders.

DHS is committed to advancing the resiliency of the Government's cyber posture to better secure Federal Executive Branch civilian systems. DHS has a number of initiatives under way that I will discuss with you today. Before I move onto the initiatives, let me emphasize, for the record, privacy and civil liberties considerations are at the center of our efforts. Protecting privacy and ensuring the proper use of personally identifiable

information is not just a priority; it is required by law and something we take very seriously.

Securing Our Federal Networks

US-CERT has been identified by the Office of Management and Budget (OMB) as the central Federal information security incident center required by the Federal Information Security Management Act of 2002 (FISMA) and serves as the operational center for the security of cyberspace of Federal Executive Branch civilian networks and CIKR networks. Agencies report incidents to US-CERT, including the identification of malicious code, denial of service, improper usage, as well as incidents that involve Personally Identifiable Information (PII). Operating a 24/7/365 operations center, the US-CERT is the lead entity in the national effort to provide timely technical assistance to operators of agency information systems regarding cyber security incidents. In this capacity the US-CERT guides agencies on detecting and handling information security incidents, compiles and analyzes information about incidents that threaten information security, and informs operators of agency information systems about current and potential information security threats, and vulnerabilities.

US-CERT, working with OMB, is building additional capacity to fulfill its responsibilities under FISMA, as well as to better protect the Federal Executive Branch civilian systems and networks or “.gov.” As a means of securing these networks, DHS is focused on implementing the Trusted Internet Connection (TIC) Initiative, which is led by the Office of Management and Budget. In addition, DHS is enhancing its EINSTEIN system, an intrusion detection capability, and deploying it at TICs across the Federal Government and at Networx Managed Trusted Internet Protocol Service (MTIPS) locations. Both of these programs support the efforts of the US-CERT—our 24/7/365 operations center that provides early watch, warning, and detection capabilities that enable us to more swiftly to identify and respond to malicious activity and to coordinate with our public and private sector partners.

The TIC initiative is a multi-faceted program which seeks to improve the U.S. Government’s cybersecurity posture and build capacity to respond to incidents by reducing and consolidating the number of external connections which Federal Executive agencies have to the Internet. The multitude of external access points gives our adversaries too many avenues to seek out vulnerabilities and exploit potential security gaps in our networks. By limiting the number of entranceways into our networks to a smaller number, we can better monitor traffic entering and exiting the network and more rapidly identify when it is penetrated by an attacker.

During this process, the U.S. Government has learned a great deal about the Federal networks. We initially identified more than 4,500 external access points, including Internet points of presence, across the Federal Government. Over the past year, departments and agencies have reduced that number. While it is important for the Government to reduce external access points, we also must ensure configuration management of the technical architecture. Through the DHS-led multiagency TIC

technical working group, comprised of TIC Access Providers, we are working to develop and implement a standard technical architecture for perimeter security which is tested through the DHS TIC compliance validation process.

Consolidating external connections and configuration management are the first step to creating a front line of defense. As we reduce external connections, we will deploy the EINSTEIN system at those TIC locations. This will allow us to more effectively analyze activity across Federal Executive Branch civilian networks. The EINSTEIN system helps to identify unusual network traffic patterns and trends that signal unauthorized network activity, allowing US-CERT to identify and respond to potential threats. DHS installed the first TIC on its own network and deployed the upgraded EINSTEIN 2 system. We will be using the lessons learned from our implementation process to assist other departments and agencies as we continue to build more TIC locations and install more EINSTEIN 2 systems.

In addition to installing the EINSTEIN 2 system on DHS's network, we created the National Cybersecurity Protection System (NCPS) to create the framework under which EINSTEIN 2 and future upgrades will be developed and deployed. NCPS is part of the overall formal acquisition program developed to enable the acquisition of technology that supports the NCSD mission including US-CERT and CNCI-related tasking.

NCPS supports the acquisition and deployment of EINSTEIN 2. We have created a plan for EINSTEIN 2 deployment that includes four phases each with the following status:

- Phase 1 – DHS Deployment: Deployment is complete and operating at initial operating capability.
- Phase 2 – Deployment at five selected Departments or Agencies: Deployment has been completed and DHS expects initial operating capability at these locations in June 2009. Technical discussions for deployment and installation of the EINSTEIN 2 system at the final Phase 2 location are ongoing.
- Phase 3 – Deployment at Networx/MTIPS Vendor Sites: Conducted technical discussions with each of the Networx/MTIPS contract awarded vendors. As the vendors complete their technical architectures, DHS is providing the EINSTEIN 2 capability and working with departments and agencies on implementation. DHS has commenced installation activities with one MTIPS awarded vendor.
- Phase 4 – Deploy to remaining Single Service TIC Access Provider Departments or Agencies: Technical discussions have begun with some of the remaining agencies. Deployments will occur as these agencies become more technically stable in their TIC implementations.

In the future, NCPS will provide US-CERT analysts with an automated capability to better aggregate, correlate, and visualize information. In addition, DHS envisions developing an Intrusion Prevention System, EINSTEIN 3, for Federal Executive Branch networks and systems. The system once fully deployed will provide the Government

with an early warning system and situational awareness, near real-time identification of malicious activity, and a more comprehensive network defense.

Together, TIC's reduction of Internet access points and EINSTEIN's situational awareness capabilities are examples of two of DHS's key initiatives designed to secure Federal networks. The eventual expansion of the EINSTEIN system, to include intrusion prevention, will create an environment that will make it more difficult, more time-consuming, and more expensive for our cyber adversaries to reach our Federal networks.

US-CERT is also taking additional steps to improve its capabilities and better protect the Federal enterprise in response to the growing threat. We recently hired additional personnel to advance US-CERT's capacity to improve information sharing and help Government and industry analyze and respond to cyber threats and vulnerabilities. This will further enable us to respond more rapidly and mitigate damage when attacks do occur. Work is also ongoing to improve collaboration with Federal departments and agencies. For example, US-CERT recently developed the Joint Agency Cyber Knowledge Exchange (JACKE) to improve situational awareness and recommend actions for Federal agency security operation centers. We are actively looking to expand the participation of the JACKE program to include all 26 major departments and agencies.

Working with the National Institute of Standards and Technology, DHS has established the US National Vulnerability Database, the government's repository of standard reference data on computer vulnerabilities. Its data is built upon the NIST Security Content Automation Protocol which enables NVD data to be used by commercial products for standardization and automation of vulnerability management, measurement, and technical policy compliance checking.

Defending Against a Full Spectrum of Threats

Globalization of the commercial information and communications technology marketplace provides increased opportunities for those bent on doing the United States harm by penetrating our supply chain and poisoning critical software and hardware. We need to make sure that products do not contain malicious code embedded in hardware or software that could compromise our systems and help our adversaries gain valuable national security information or disrupt our networks. Thus, it is imperative that we work towards a stronger supply chain defense to reduce the potential for adversaries to manipulate our information technology and communications products before they are installed.

Protecting U.S. Government networks through global supply chain risk management requires a multi-pronged approach. DHS and the DoD have formed a partnership to coordinate supply chain risk management (SCRM) activities in the Government. DHS has taken responsibility for non-national security related systems, while DoD is responsible for national security systems. Addressing this risk requires greater awareness of threats, vulnerabilities, and consequences. It will also require sound acquisition policies and practices, and will require the adoption of supply chain and risk

managements standards and best practices. We are working with the National Institute of Standards and Technology and several other agencies towards the long-term goal of enhancing Federal Government skills and capabilities, and to provide departments and agencies with the necessary toolsets to better manage and mitigate supply chain risk.

The DHS SCRM Program will improve our capabilities through conducting SCRM pilots and establishing formal working groups within the Government and private sector to inform program activities. The program is structured to meet requirements through testing, counterintelligence risk methodologies, best practices, controls, and other elements of supply chain risk management. Finally, enhancing our public-private partnership is essential, as the Federal Government cannot by itself ensure the integrity of the supply chain.

Leveraging \ Partnerships

Key to succeeding in protecting our cyber infrastructure is collaboration with the private sector. As previously noted, most of our critical infrastructure and the Nation's cyber networks are owned and operated by private industry. Thus, a comprehensive, holistic cybersecurity strategy cannot be successful without an intensive engagement and collaboration with the private sector. Both government and private sectors have much to gain from working and sharing information with one another. The creation of a strong partnership between these two sectors will help greatly in securing our cyber systems.

One of the initiatives under the CNCI was dedicated to improving protection of privately owned critical network infrastructure through public private partnership (Project 12). This is one of the ways DHS is trying work with the private sector to improve and institutionalize information sharing. As a part of this initiative, we are also looking to increase our public-private information sharing and coordination efforts and are engaging in discussions with the private sector to encourage collaboration with the business community nationwide. These discussions serve as information forums for businesses to better understand the cyber threats identified by Government and for Government to understand better the private sector's prodigious cybersecurity capabilities. This bi-directional information flow is crucial. DHS is also working to leverage the good work that DoD has done with the defense industrial base sector to increase actionable bi-directional information sharing of real and usable information with other sectors.

State, local, tribal governments and international communities also play crucial roles in improving the U.S. cybersecurity posture. Recognizing the contributions that can be made by leveraging such partnerships, DHS is working with all levels of government across the nation to help increase awareness regarding cybersecurity and related preparedness and response issues. Specifically, DHS provides technical and operational assistance to State cybersecurity partners to assist in planning and executing cyber exercises. To expand this effort, NCSD is developing a repeatable cyber exercise assistance program that will be deployed to assist states with their cyber exercise needs. This program will include background and educational materials, the potential for a "train

the cyber exercise trainer” program, staff and technical assistance with developing and executing exercises, as well as tools and resources to build upon past exercise efforts, and to integrate into future efforts such as the Cyber Storm Exercise series.

Cyber threats do not stop at traditional physical boundaries, so DHS collaborates with the international community to manage global cyber risk. In coordination with the our Federal partners, we are engaging both with multilateral organizations and in multilateral forums, such as the European Union, the Group of 8, and the Meridian Conference, to enhance information sharing and situational awareness, improve incident response capabilities and coordinate on strategic policy issues.

Cybersecurity Workforce Education: Improving and Maintaining Our Workforce

In addition to being responsible for advances in our cybersecurity posture, DHS is working with other agencies to develop a plan for the retention of a skilled, trained workforce. Our adversaries are skilled and motivated, requiring us to constantly stay one step ahead of their actions. In order to address cybersecurity challenges, we need to build the next generation of our cybersecurity workforce that will help us develop a competitive advantage. Thus, we are focusing our resources on education and training of our current workforce, as well as recruiting new talent in order to develop a world-class workforce. DHS is also encouraging university programs and providing scholarships to promising students.

DHS believes that workforce development is critically important to our cybersecurity mission. DHS is actively recruiting and looking to fill new cybersecurity positions at NCSD. These positions range from entry level to management. For example, increases to US-CERT’s staff, as DHS’s watch and warning center, greatly enhance its ability and capacity for preparedness and response activities. We are actively recruiting for these open positions in order to improve our capabilities and expand our core leadership team.

Beyond the Government domain, DHS is focusing its efforts on providing individuals within the cybersecurity sector of private industry with a baseline set of cyber skills. To achieve this, DHS worked across the public and private sector to develop the first Information Technology Security Essential Body of Knowledge to provide the cybersecurity community with the baseline skills and knowledge all information technology security professionals should possess to successfully perform their jobs. Cybersecurity is the responsibility of us all. Thus, we are striving to minimize our cyber gaps and vulnerabilities through both top-down and bottom-up approaches.

As part of our shared responsibility, we cannot simply focus on the present. We must also look to the future. This requires us to not only shape the workforce, but the community of computer users as well. Cybersecurity and cyber safety are learned behaviors, and we need to teach children how to be secure online. Here we are building from the ground up. By teaching children skills at a young age, we are laying the foundation from which our future cybersecurity workforce will come, while

simultaneously improving our cyber defense. DHS is working with the National Cybersecurity Alliance (NCSA) to make this vision a reality. In addition to ongoing work with the K-12 community, the NCSA recently launched its Cybersecurity Awareness Volunteer Education (C-SAVE) Project. This program encourages security professionals to put their knowledge and expertise to work in their local schools and help fill a tremendous gap in educating young people to use the Internet securely and safely. We are very pleased to be working with the NCSA on this program as this is a crucial endeavor to ensure the continued success and advancement of our cybersecurity mission.

White House Cyberspace Policy Review

On February 17, 2009, President Obama initiated a White House Cyberspace Policy Review of cybersecurity policies and issues affecting the Nation. On May 29, 2009, the results of that review were published by the White House in a report entitled *Assuring a Trusted and Resilient Information and Communications Infrastructure*. The review solidified the priority that the Administration places on improving the Nation's cybersecurity, and DHS will continue to have a key role as the lead agency for securing Federal Executive Branch civilian networks and collaborating with the private sector to enhance the cybersecurity of non-Federal CIKR networks.

DHS will have a significant role in several near-term actions outlined in the report, including updating the national strategy, strengthening international partnerships, increasing public awareness, and preparing a national response plan for cyber incidents. These near-term actions will enable DHS in collaboration with its government and industry partners to continue to address the growing and evolving cyber threat. Additionally, the operational goals of the comprehensive national strategy will include better coordination, response, recovery, and mitigation capacity across all stakeholder communities.

Conclusion

The cyber threat is rapidly growing and evolving. As the Nation becomes ever more dependent upon cyber networks, we must address cybersecurity swiftly and surely. Overcoming new cybersecurity challenges is a difficult task requiring a coordinated, focused approach to better secure the Nation's information technology and communications infrastructures. Accordingly, DHS is actively working with its Federal partners to secure the ".gov" domain by implementing a holistic strategy for securing our civilian networks and systems.

Through government-wide programs such as TIC and EINSTEIN, we are enhancing the Government's cybersecurity posture by reducing the number of external connections, including connections to the internet, while improving our detection and response

capabilities. We are also striving to create a strong supply chain defense and develop an enduring, robust workforce.

It cannot be over-emphasized that, while DHS is focused on developing the necessary analytical, response, and technical capabilities to create a comprehensive network defense to secure the Nation's CIKR, we are not in this alone. A truly comprehensive cyber strategy requires an open partnership with the private sector, and it is in this arena that we are continually working to advance our mission. Everyone plays a role in cybersecurity, from the Federal, State, local, tribal and international governments to the private sector to the citizens who access computers for personal use. DHS is committed to its cybersecurity mission and will continue to reach out to these parties to promote cyber awareness, identify best practices, mitigate risks and improve its ability to respond to cyber incidents. The Department is also actively pursuing avenues to further collaboration and information sharing with these partners. The developments DHS has made in strengthening Federal systems, enhancing our operational cyber response capabilities, and strengthening the public-private partnership have been significant, but we are committed to doing more.

Thank you for your time today. I appreciate the opportunity to discuss the Department's efforts in advancing our cybersecurity posture and increasing our security of Federal networks. I will be happy to answer any questions from the Subcommittees.