Statement for the Record
of
Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

June 15, 2010

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is an honor to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. I appreciate the opportunity to testify today regarding the critical issue of cybersecurity, and to discuss some of the major aspects of the Protecting Cyberspace as a National Asset Act.

The President has described our networks, and the hardware that supports them, as "strategic national assets" and called the growing number of attacks on these networks "one of the most serious economic and national security threats our nation faces." The President has also clearly laid out the roles and responsibilities for protecting nationally critical civilian networks:

- DHS has the lead to secure federal civilian systems, sometimes described as the dot-gov domain.
- DHS works with critical infrastructure and key resources (CIKR) owners and operators—whether private sector, state, or municipality-owned—to bolster their cyber security preparedness, risk mitigation, and incident response capabilities.

With that in mind, I would like to begin with a few key points.

- First, this cybersecurity endeavor is not just about DHS. The mission is for the entire homeland security enterprise, which includes many agencies, such as DHS, and the Departments of Commerce, State, Justice, and Defense. DHS will continue to play a critical role because of its responsibility to secure federal civilian networks and its mission to protect CIKR, both physical and cyber, in close coordination with the private sector and state governments but is actively engaged with its sister agencies on public policy and operational challenges that might impinge upon our nation's cybersecurity.
- Second, in response to the President's call to action a year ago, DHS has been focused on addressing an increasingly threatening cyber environment. We are fulfilling our mission responsibilities and challenging the status quo.

- Third, DHS is vigorously developing new capabilities, increasing response capacity, organizing for future successes, and bolstering security in both the public and private sectors.
- Fourth, there is no silver bullet to cybersecurity; we must employ a defense-in-depth approach. We are bringing in the technology and capabilities that the private sector has to offer, and we are encouraging and promoting innovation and creativity in order to achieve increased security and resiliency.

Mr. Chairman, the United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

As bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We can never be certain that our information infrastructure will remain accessible and reliable during a time of crisis, but we can reduce the risks.

We face persistent and unauthorized intrusions to federal executive branch civilian networks that often are difficult to attribute. These intruders may be nation state actors, terrorists, organized criminal groups, or individuals located here in the United States or abroad. They have varying levels of access and technical sophistication, but all have nefarious intent. Many are capable of targeting elements of the U.S. information infrastructure to disrupt, dismantle, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, and disruption of economic stability. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. Terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own technical abilities, of equal concern is the wide availability of advanced technical tools for purchase or for free off the Internet.

In the virtual world of cyberspace, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten our economic well being and national security, critical infrastructure, public health and welfare, privacy, civil rights and civil liberties, and confidence in government. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure, and at their time of greatest advantage. Securing cyberspace is similar to protecting physical borders and ports, enforcing and facilitating the immigration laws, securing the aviation and surface transportation system, and preparing to respond from both natural and manmade events: it requires a defense-in-depth approach. Indeed, securing cyberspace is also critical to accomplishing the physical security missions of protecting borders and ports, enforcing immigration laws, aviation security, and responding to natural and

manmade events successfully because of the mutual dependence and interconnected nature of the cyber and physical security missions and efforts.

In cyberspace, just as in physical domains, we need to ensure that Federal systems are secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from causing harm. Further, we must use our knowledge of these systems and their interdependencies to prepare to respond should our protective efforts fail. This is a serious challenge, and DHS has made great progress over the past year to improve the nation's overall operational posture and forward-looking policy efforts.

Overview of DHS Cybersecurity Responsibilities

DHS is responsible for helping federal executive branch civilian departments and agencies to secure their unclassified networks, often called the dot-gov domain. DHS also works closely with partners across government and in industry assisting them with the protection of private sector critical infrastructure networks. The Department has a number of foundational and forward-looking efforts under way, many of which stem from the Comprehensive National Cybersecurity Initiative (CNCI).

The CNCI comprises a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- Establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- Defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- Strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the federal government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

DHS plays a key role in many of the activities supporting these goals and works closely with our federal partners to secure our critical information infrastructure in a number of ways. We are reducing and consolidating the number of external connections federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to those TICs. Through the United States Computer Emergency Readiness Team (US-CERT), we are working more closely than ever with our partners in the private sector and across the federal government to share what we learn from our EINSTEIN deployments and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. In addition, the Department has a role in the Federal Government for cybersecurity research and development (R&D). The DHS Science and Technology (S&T) Directorate's Cyber Security R&D (CSRD) program funds activities addressing core vulnerabilities in the Internet, finding and eliminating malicious

software in operational networks and hosts, and detecting and defending against large scale attacks and emerging threats on our country's critical infrastructures. The CSRD program includes the full R&D lifecycle -- research, development, testing, evaluation, and transition -- to produce unclassified solutions that can be implemented in both the public and private sectors. The S&T Directorate has established a nationally recognized cyber security R&D portfolio addressing many of today's most pressing cybersecurity challenges. The CSRD program has funded research that today is realized in more than 18 open-source and commercial products that provide capabilities, including the following: secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis, and security for process control systems.

President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader national cybersecurity strategy. These CNCI initiatives and its associated activities will play the central role in implementing many of the key recommendations of President Obama's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.

With the publication of the *Cyberspace Policy Review* on May 29, 2009, DHS and its components have developed a long-range vision of cybersecurity for the Department's—and the nation's—homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions, as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: to help create a safe, secure, and resilient cyber environment, and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano has consolidated the Department's cybersecurity efforts under the coordination of the National Protection and Programs Directorate (NPPD) and in my role as the Director of the National Cyber Security Center. We are moving aggressively to build a world-class cybersecurity team, and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats. Most immediately, we are focusing on three priorities:

1. Continue enhancement of the EINSTEIN system's capabilities as a critical tool in protecting our federal executive branch civilian departments and agencies.
2. Develop the National Cyber Incident Response Plan (NCIRP) in full collaboration with the private sector and other key stakeholders. The NCIRP will ensure that all national cybersecurity partners understand their roles in cyber incident response and are prepared to participate in a coordinated and managed process. The NCIRP will be tested this fall during the Cyber Storm III National Cyber Exercise.
3. Increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

DHS also bears primary responsibility for raising public awareness about threats to our nation's cyber systems and networks. Every October DHS in coordination with other federal agencies, governments and private industry, make a concerted effort to educate and inform the public through the National Cybersecurity Awareness Month (NCSAM) campaign, and we are making progress. For example, in 2009, the Secretary of Homeland Security and the Deputy Secretary of Defense jointly opened the campaign, we engaged in our most significant outreach ever, and all 50 states, the District of Columbia, and the U.S. Territory of American Samoa, as well as seven tribal governments, endorsed NCSAM.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency or even solely within the Federal realm; it requires teamwork and coordination across all sectors because it touches every aspect of our lives. Together, we can leverage resources, personnel, and skill sets that are needed to accomplish the cybersecurity mission. The fiscal year (FY) 2011 NPPD budget request for cybersecurity strengthens the ongoing work in each of the Department's offices to fulfill our unified mission.

The Office of Cybersecurity and Communications (CS&C), a component of NPPD, is focused on reducing risk to the nation's communications and IT infrastructures and the sectors that depend upon them, and enabling timely response and recovery of these infrastructures under all circumstances. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C is comprised of three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

NCSD collaborates with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructure. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' responsibilities under the CNCI.

Within NCSD, US-CERT leverages technical competencies in federal network operations and threat analysis centers to develop knowledge and knowledge-management practices. NCSD provides a single, accountable focal point to support federal stakeholders as they make key operational and implementation decisions to secure the federal executive branch civilian networks. It is through NCSD's programs that the Trusted Internet Connections Initiative and the National Cybersecurity and Protection System, which I will discuss later, are implemented and upon which stakeholders look to for support during steady-state and crisis. NCSD takes a holistic approach enabling federal stakeholders to address cybersecurity challenges in a manner that maximizes value while minimizing risks associated with technology and security investments. Further, NCSD through US-CERT analyzes threats and vulnerabilities, disseminates cyber threat warning information, and coordinates with partners and customers to achieve shared situational awareness related to the nation's cyber infrastructure.

As I mentioned before, the Department is responsible for supporting federal executive branch civilian agencies in the protection and defense of their networks and systems. The Department's strategy, which supports a defense-in-depth, requires situational awareness of the state of federal networks, an early warning capability, near real-time and automatic identification of malicious activity, and the ability to disable intrusions before harm is done. DHS, through NCSD and US-CERT, developed a "system-of-systems" approach to support its cybersecurity mission (noted above). This overall system-of-systems is known as the National Cybersecurity Protection System (NCPS). As part of the NCPS, DHS is deploying a customized intrusion detection system, known as EINSTEIN 2, to federal executive branch civilian agencies to assist them in protecting their computers, networks, and information.

None of this is possible, however, without a comprehensive understanding of federal executive branch civilian networks from an enterprise perspective. The CNCI TIC initiative provides the federal government this understanding by reducing and consolidating external access points across the federal enterprise, assisting with the security requirements for federal agency network and security operations centers, and establishing a compliance program to monitor federal agency adherence to TIC policies.

The Department is installing EINSTEIN 2 capabilities on federal executive branch civilian networks in distinct but interconnected steps. The first step, under the TIC initiative, is the consolidation of external connections and application of appropriate protections thereto. This will help create an efficient and manageable front line of defense for federal executive branch civilian networks. The goal is to get down to less than 100 physical locations. Our program office has been working with departments and agencies to better understand how civilian agencies configure their external connections, including Internet access points, and improve security for those connections. As departments and agencies are consolidating their external connections, we are working to deploy EINSTEIN 2 to these TIC locations to monitor incoming and outgoing traffic for malicious activity directed toward the federal executive branch's civilian unclassified computer networks and systems. EINSTEIN 2 uses passive sensors to identify when unauthorized users attempt to gain access to those networks. EINSTEIN 2 is currently deployed and operational at 11 of 19 departments and agencies. The EINSTEIN 2 system is already providing us with, on average, visibility into more than 278,000 indicators of potentially malicious activity per month.

The TIC initiative and EINSTEIN 2 deployments are critical pieces of the federal government's defense-in-depth cybersecurity strategy. DHS is also building upon the enhanced situational awareness that EINSTEIN 2 provides. We currently are working with the private sector, the National Security Agency, and a wide range of other federal partners to test the technology for the third phase of EINSTEIN, an intrusion-prevention system which will provide DHS with the capability to automatically detect malicious activity and disable attempted intrusions before harm is done to our critical networks and systems.

For all these deployments, it is important to note that EINSTEIN capabilities are being carefully designed in close consultation with civil liberties and privacy experts—protecting civil liberties and privacy remains fundamental to all of our efforts.

These accomplishments are reliant upon increasing the number of dedicated and skilled people at CS&C. To this end, the National Cyber Security Division tripled its federal workforce from 35 to 118 in FY 2009, and we hope to more than double that number to 260 in FY 2010. We are moving aggressively to build a world-class cybersecurity team, and we are focusing on key priorities that address people, processes, and technology.

Recently, the Office of Management and Budget (OMB) and the President's Cybersecurity Coordinator issued new Federal Information Security Management Act (FISMA) reporting requirements that will help our cybersecurity workforce to inculcate a culture of cyber safety. The new requirements are designed to shift efforts away from compliance on paper and towards implementing solutions that actually improve cybersecurity. The new reporting requirements will automate security-related activities and incorporate tools that correlate and analyze information, giving the government's cyber leaders manageable and actionable information that will enable timely decision-making. DHS will provide additional operational support to agencies in securing their networks by monitoring and reporting agency progress to ensure the new OMB/ Cybersecurity Office guidance is effectively implemented. This new reporting follows a three-tiered approach:

- Data feeds directly from security management tools—agencies are already required to report most of this information. It includes summary information on areas such as inventory, systems and services, hardware, software, and external connections.
- Government-wide benchmarking on security posture—which will help to determine the adequacy and effectiveness of information security, civil rights and civil liberties, and privacy policies, procedures, and practices throughout the government.
- Agency-specific interviews—which will be focused on specific threats each agency faces and will inform the official FISMA report to Congress.

Response to Legislation

DHS welcomes working with the Committee on strengthening the Department's ability to accomplish its cybersecurity mission—securing federal executive branch civilian systems and working with the private sector and federal sector-specific agencies to secure the nation's CIKR.

- We appreciate support for DHS' mission in implementing cybersecurity for federal civilian networks, working in partnership with the private sector to secure critical infrastructure systems and functions.
- The Department is looking to maximize its hiring flexibilities in support of fulfilling its cyber mission.
- The Administration currently is reviewing the appropriate scope of authority to ensure that the Department's cybersecurity mission can be achieved, and we look forward to continuing to work with Congress in this regard. Regulatory agencies in sectors such as banking, finance, energy, transportation, healthcare, and communications should continue to review existing cybersecurity regulatory requirements and determine if new rulemaking is required. These sectors should continue to consult with DHS and the National Institute for Standards and Technology during this process.
- The bill recognizes that Americans expect the federal government to anticipate, prevent, and respond to cyber threats. The provisions relating to imminent cyber threats acknowledge that the government may need to take extraordinary measures to fulfill these responsibilities.

Section 706 of the Communications Act and other laws already address Presidential emergency authorities and Congress and the Administration should work together to identify any needed adjustments to the Act, as opposed to developing overlapping legislation. We will continue to assess this issue and others that touch on the relationship between government and the private sector.

- DHS also welcomes the fact that this legislation ensures that privacy and civil liberties protections will continue to be fully integrated into our cybersecurity operations.
- With regard to the revised FISMA provisions, the Administration has begun significant FISMA reform that streamlines and updates the process and increases the focus on outcomes. The Administration is developing new policy guidance to clarify the role of DHS in Federal cybersecurity activities.
- While this Committee and DHS clearly share the common goal of increasing the Department's capabilities to meet the cybersecurity mission, we believe that it is preferable to maintain a singular organizational integration between physical and cybersecurity operations, rather than create a separate cyber organization.
    - This Committee is well aware of Supervisory Control and Data Acquisition (SCADA) systems—the electronic systems that allow infrastructure owners to remotely operate our dams, our power generation plants, and our transportation networks. The NPPD Office of Infrastructure Protection empowers private and public stakeholders to protect these assets through vulnerability assessments and an active field presence. CS&C, moreover, monitors cyber-based threats and vulnerabilities that could compromise SCADA systems and also engages directly with asset owners to mitigate risk. These physical infrastructure and cybersecurity efforts are best enabled by maintaining and expanding organization connection, thus promoting efficiencies, providing expanded situational awareness, and helping to keep America running.
    - We continue to believe that the nexus point between critical (physical) infrastructure that have cybersecurity vulnerabilities, such as the electrical grid which could potentially be hacked through the Internet, can best be made resilient through a single organizational entity that works to prevent, mitigate, and recover from all-hazards attacks where the lines of cyber and physical security are erased.

Conclusion

Mr. Chairman, Ranking Member Collins, Members of the Committee, thank you again for your strong support of the Department, and for your dedication to improving cybersecurity. We look forward to working with you to strengthen efforts that are critical to the nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the nation and keep Americans safe.

Thank you for again for this opportunity to testify. I would be happy to answer any of your questions.