Statement for the Record
of
Gregory Schaffer
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Washington, DC

June 16, 2010

Introduction

Mr. Chairman, Ranking Member King, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. I will provide an update on our efforts to better solidify the federal executive branch civilian networks and systems, critical infrastructure, and our public-private partnerships. At the Department, our efforts are focused on enhancing the cybersecurity posture of the nation by improving our capacity to prevent, identify, respond to and recover from cyber threats.

As a nation, it is essential that we are aware of, and focused on, the cyber threat. Just as important, the government must be able to move quickly and purposefully to address cyber threats as malicious actors rapidly change techniques, technology, and tradecraft. As you know, Mr. Chairman, threats are becoming more targeted, more sophisticated, and more numerous.

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 President has described our networks, 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, in coordination with other Federal Sector-Specific Agencies as appropriate.

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 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 its Deputy Under Secretary who also serves as the Director of the National Cyber Security Center. As NPPD leadership, we are moving aggressively to build a world-class cybersecurity team, and we have identified three key priorities that enable 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, makes a concerted effort to educate 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 infrastructures. 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. US-CERT provides a single, accountable focal point to support federal stakeholders as they make key operational and implementation decisions and secure the federal executive branch civilian networks. US-CERT's holistic approach enables federal stakeholders to address cybersecurity challenges in a manner that maximizes value while minimizing risks associated with technology and security investments. Further, 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.

DHS 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 layered defense, 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), in which 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 managing 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 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. In parallel with learning about how agencies are configured, we are working with OMB and departments and agencies to consolidate their external connections and as they do that DHS is deploying 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 rights and civil liberties and privacy experts—protecting civil rights, 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, NCSD 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 certain 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 department and agency 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 will help to determine the adequacy and effectiveness of information security and privacy policies, procedures, and practices throughout the government.
- Agency-specific interviews will be focused on specific threats each agency faces and will inform the official FISMA report to Congress.

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.

Perhaps more ominously, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security as well as public health and safety or an individual's civil rights and civil liberties and privacy. Thus, while we strive to prevent loss of intellectual capital from our networks, we are also working to ensure that the systems that support the essential functions that underpin American society—critical infrastructure and key resources (CIKR)—are protected from cyber threats.

Of particular importance are those systems that operationally control our critical infrastructure, such as the energy grid and communications networks. These systems must remain accessible and reliable during times of crisis. Understanding the nexus between the physical and the cyber worlds is an essential mission area for the Department, and one that must permeate all of our efforts.

At DHS, we are very aware that some critical infrastructure elements are so vital to our nation that their destruction or incapacitation would have a debilitating impact on national security and economic well-being. We recognize that partnering with the private sector to assist in securing critical infrastructure is one of our most important missions. One key priority is DHS' control systems security program, which provides expertise, tools, and leadership to the owners of control systems. A cyber attack on a control system could result in dire physical consequences, even loss of life. We are providing operational support to the control systems community through our Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

ICS-CERT provides onsite support for incident response and forensic analysis at the request of the affected entity. It also shares and coordinates vulnerability information and threat analysis through information products and situational alerts. Through our advanced vulnerability discovery laboratory, we identify vulnerabilities in control systems and develop and distribute mitigation strategies in partnership with both private sector vendors and operators. The control system program also provides tools (such as the Cyber Security Evaluation Tool) and training to increase stakeholder awareness of the evolving risks to control systems. To date, DHS has helped train more than 14,000 control system operators in the classroom and on the web on how to deal with a variety of cyber attacks. We also created a collection of recommended practices and informational products to assist owners and operators in improving the security of their control systems.

DHS conducts site assessments of selected CIKR facilities (and encourages self-assessments by owners and operators of additional facilities) to identify vulnerabilities and recommend enhancements. In late 2009, we took steps to meet increasing industry requests by implementing a dedicated cybersecurity evaluations program that ensures vulnerabilities identified in our key cyber infrastructure are done so under a consistent and formal framework of evaluation. The program office is working closely with industry to bolster their cybersecurity preparedness, risk mitigation, and incident response capabilities. Through this direct outreach, we expect to improve our capacity to measure private sector performance in managing cybersecurity. We conduct these assessments in close partnership with NPPD's Office of Infrastructure Protection, recognizing the need to intertwine physical security with cybersecurity. In just the last few weeks, we have had teams in Washington, Massachusetts, Missouri, Arizona, and North Dakota to look at individual facilities, regional clusters of critical infrastructure, control systems, and business networks.

In addition to work done with the ICS-CERT, DHS has other efforts designed to help protect critical infrastructure and key resources. In 2006, we established the Cross-Sector Cyber Security Working Group to address cross-sector cyber risk and explore interdependencies between and among various sectors. The working group serves as a forum to bring government and the private sector together to address common cybersecurity elements across the 18 CIKR sectors. They share information and provide input to key policy documents, such as the *National Strategy for Trusted Identities in Cyberspace*. The Department conducts its critical infrastructure protection activities under the National Infrastructure Protection Plan (NIPP) framework to facilitate effective coordination between government infrastructure protection programs and the infrastructure protection and resilience activities of the owners and operators of CIKR resources.

To secure critical infrastructure, the NIPP relies on the sector partnership with the federal government. This includes Sector Coordinating Councils and their associated Information Sharing and Analysis Centers, the Homeland Security Information Network, technology and service providers, specific topical working groups, and partners from across the 18 CIKR sectors. These information-sharing mechanisms will continue to enhance and facilitate information exchange throughout the CIKR community, private sector, and government—making everyone's networks and systems more secure.

The Information Technology Sector Baseline Risk Assessment (ITSRA) is an example of public and private sector information sharing. The completion of the ITSRA last fall was a significant milestone for both the NIPP sector partnership model and for the IT Sector Specific Plan implementation. This important effort identifies strategic and national-level risks to the IT sector and will inform risk management activities across the IT sector this year. It will also focus additional attention on important cross-sector IT risk-related dependencies and inform both government and industry mitigations, research and development priorities, and resource decisions.

In this sense, it is a true force multiplier in that many sectors are apt to benefit from the IT sector's close working relationship with the public sector. DHS will continue to work with IT sector partners to use the IT sector risk management methodology to identify appropriate responses for the risks identified for each IT sector critical function. This will prioritize mitigation activities and inform corresponding risk management strategies to provide the greatest reduction to the national level risks identified in the ITSRA. The 2010 Communications Sector Risk Assessment, which is currently under way, will outline security measures that will better support business operations and form the basis of meaningful infrastructure protection metrics. This assessment will complement the ITSRA's functions-based approach and augment its 2008 assessment.

As we move forward, public-private cooperation is growing ever more important. We are building on already successful partnerships and looking forward to new opportunities. DHS is moving toward greater, more actionable sharing of information with the private sector based on new analytical insights derived from a comprehensive understanding of the government-wide cyber domain. DHS has initiated several pilot programs that enable the mutual sharing of cybersecurity information at various classification levels:

- DHS and Michigan are conducting a proof-of-concept pilot in which the EINSTEIN 1 network flow monitoring technology helps secure Michigan's dot-gov networks. The purpose of this study is to help state governments enhance their cybersecurity and to increase DHS overall cyber situational awareness.
- DHS, the Department of Defense (DOD), and the Financial Services Information Sharing and Analysis Center have launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information—in both directions—to mitigate the impact of attempted cyber intrusions. This builds on the products and success of DOD's Defense Industrial Base initiative. This pilot is currently at the For Official Use Only level, but shortly will be enhanced to include Secret-level information.
- We are also working on a pilot that brings together state fusion centers and private sector owners and operators of critical infrastructure to provide access to Secret-level classified cybersecurity information. The Cybersecurity Partners Local Access Plan is a pilot initiative allowing security-cleared owners and operators of CIKR, as well as State Chief Information Security Officers and Chief Information Officers, to access Secret-level cybersecurity information and participate in Secret-level video teleconference calls via their local fusion centers, allowing classified information sharing outside of Washington, D.C.
- DHS has instituted a Top Secret/Sensitive Compartmented Information clearance program for CIKR representatives to enable their engagement in analysis of the most sensitive cybersecurity threat information.

The Department also is working in the areas of software assurance and supply chain management so that government and private sector partners can work together to solve what is a potentially serious security issue. We believe software developers must automate security and institutionalize it from the beginning in an effort to change the current security posture from reactive to proactive.

Shifting to a proactive posture will also help prevent threats from entering our critical systems and networks, to which end software assurance and supply chain management are so vitally important. By definition, the private sector will have the largest role in developing solutions for more secure software and in supply chain management. To be sure, the government can help by driving security requirements, but we need to be creative and collaborative in developing partnerships between and among the private and public sector cyber communities to exchange information and ideas.

We need to develop a cybersecurity culture that realizes that everyone—government, corporate, or private—has a vested stake in all aspects of cybersecurity. For example, we need to evaluate and reflect upon each software failure and break in the supply chain to gain greater process insights and develop long-term software assurance and supply chain management solutions. To do this, we will need to authenticate people, processes, and devices. In other words, we need to develop inherently secure business practices in supplying critical products. In terms of software, this means we need mechanisms that allow computer code to stand on its own merits and speak for itself.

As I mentioned earlier, DHS is taking steps to improve the overall cybersecurity posture of the nation. Our approach interlocks strategically with other efforts that are ongoing across the federal government, private sector and across the country in states and localities. One of our most important initiatives is our effort to improve cybersecurity incident handling and response processes via the National Cyber Incident Response Plan, or NCIRP. The goal of the NCIRP is to build upon the concepts and methodologies of the National Response Framework, the National Incident Management System, and the NIPP. This is an interagency effort in coordination with state, local, tribal and private sector partners to define the cyber incident roles and responsibilities across a wide spectrum of stakeholders. The plan will provide federal agencies; state, local and tribal governments; and the private sector with a better understanding of how to respond to a cyber event during a crisis or under normal operating conditions. We will test the plan during the Cyber Storm III National Cyber Exercise this fall.

The NCIRP will be crucial for effective incident response, which will leverage the strength of our new operations center. During the first quarter of FY 2010, DHS launched the National Cybersecurity and Communications Integration Center (NCCIC), a facility that improves our capability and capacity to detect, prevent, respond, and mitigate disruptions of the nation’s cyber and communications systems. The NCCIC collocates vital IT and communications operations centers, thereby converging existing incident response mechanisms and better reflecting the reality of technological convergence. Under the NIPP partnership framework, the collaborative activity of the NCCIC blends together the interdependent missions of the National Coordinating Center for Telecommunications, US-CERT, the DHS Office of Intelligence and Analysis, and the National Cyber Security Center. We are working through the legal and operational details to enable the planned inclusion of private sector representation on the NCCIC floor.

Conclusion

I appreciate the opportunity to speak with you today about the progress that the Department has made and the road ahead for future improvements to our nation's cybersecurity. DHS is committed to working collaboratively with our public, private, academic, and interagency partners to ensure that the cyber elements of our nation's critical infrastructure are secure. We strive to ensure that these systems are robust enough to withstand attacks, responsive enough to recover from attacks, and resilient enough to sustain critical operations. We will continue to build upon our efforts and create more effective partnership opportunities that will allow us to make our nation's critical infrastructure safer and more secure.

Again, thank you for this opportunity to testify. I would be happy to answer any questions you may have.