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

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Washington, DC

March 16, 2011

Introduction

Chairman Lungren, Vice Chairman Walberg, Ranking Member Clarke, and distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. I will provide an overview of the current cybersecurity environment, the Department's cybersecurity mission as it relates to critical infrastructure, and the coordination of this mission with our public and private sector partners.

We would like to work more with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on for daily life, such as water distribution and treatment, electricity generation and transmission, healthcare, transportation, and financial transactions depend on an underlying information technology and communications infrastructure. Cyber threats put the availability and security of these and other services at risk.

The Current Cybersecurity Environment

The United States confronts a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of 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 and the information collection and sharing process, and as bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We currently cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis.

We face persistent, unauthorized, and often unattributed intrusions into Federal Executive Branch civilian networks. These intruders span a spectrum of malicious actors, including nation states, terrorist networks, organized criminal groups, or individuals located here in the United States. They have varying levels of access and technical sophistication, but all have nefarious

intent. Several 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, or disruption of commercial activities, among others. 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. In addition, 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 lack of technical abilities, the availability of technical tools for purchase and use remains a potential threat.

Malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security, critical infrastructure, public health and welfare, 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 requires a layered security approach. Moreover, securing cyberspace is also critical to accomplishing nearly all of DHS's other missions successfully.

We need to support the efforts of our state and local government and private sector partners to secure themselves against malicious activity in cyberspace. Similarly, we need to ensure that the federal civilian environment is secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from penetrating our defenses. Collaboratively, public and private sector partners must use our knowledge of these systems and their interdependencies to prepare to respond should defensive efforts fail. This is a serious challenge, and DHS is continually making strides to improve the nation's overall operational posture and policy efforts. In addition, other departments, such as the Department of Education, are working to educate parents and students on Internet safety and privacy protection.

Cybersecurity Mission

Let me be clear that no single technology – or single government entity – alone can overcome the cybersecurity challenges our nation faces. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort between the private sector, critical infrastructure owners and operators, and the extensive expertise that lies across coordinated government entities. The National Protection and Programs Directorate (NPPD) within DHS is responsible for the following key cybersecurity missions:

- Leading the effort to secure Federal Executive Branch civilian departments and agencies' unclassified networks;
- Providing technical expertise to the private sector and critical infrastructure and key resources (CIKR) owners and operators—whether private sector, state or municipality-owned—to bolster their cybersecurity preparedness, risk assessment, mitigation and incident response capabilities;
- Raising cybersecurity awareness among the general public; and
- Coordinating the national response to domestic cyber emergencies.
- Leveraging cyber defense capability across all departments and agencies to detect, respond, isolate and remediate cyber attacks or practices dangerous to security and privacy.

In a reflection of the bipartisan nature with which the federal government continues to approach cybersecurity, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated activities should evolve to become key elements of the broader national cybersecurity efforts. These CNCI initiatives play a central role in achieving many of the key recommendations of the President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Following the publication of those recommendations in May 2009, DHS and its components developed a long-range vision of cybersecurity for the Department and the nation's homeland security enterprise, which is encapsulated in the Quadrennial Homeland Security Review (QHSR). The QHSR provides an overarching framework for the Department and defines our key priorities and goals. One of the five priority areas detailed in the QHSR is safeguarding and securing cyberspace. Within the cybersecurity mission area, the QHSR identifies 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 consolidated many of the Department's cybersecurity efforts under NPPD. The Office of Cybersecurity and Communications (CS&C), a component of NPPD, focuses on reducing risk to the nation's communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. The functions and mission of the National Cybersecurity Center (NCSC) are now supported by CS&C. These functions include coordinating operations among the six largest federal cyber centers. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C comprises three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System. Within NCSD, the United States Computer Emergency Readiness Team (US-CERT) is working more closely than ever with our public and private sector partners to share what we learn from EINSTEIN 2, a federal executive agency computer network intrusion detection system, to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. EINSTEIN enables us to respond proactively to warnings and other indicators of operational cyber attacks, and we have many examples showing that this program investment has paid for itself several times over.

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; it requires teamwork and coordination. Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace.

NCSD collaborates with federal government stakeholders, including civilian agencies, law enforcement, the military, the intelligence community, state and local partners, and private sector stakeholders, to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of civilian government and private sector critical 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' non-law enforcement cybersecurity responsibilities.

National Cyber Incident Response

The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan. The plan provides a framework for effective incident response capabilities and coordination among federal agencies, state and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines. In September 2010, DHS hosted Cyber Storm III, a response exercise in which members of the domestic and international cyber incident response community addressed the scenario of a coordinated cyber event. During the event, the National Cyber Incident Response Plan was activated and its incident response framework was tested. Based on observations from the exercise, the plan is in its final stages of revision prior to publication.

Cyber Storm III also tested the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber watch and warning center—and the federal government's full suite of cybersecurity response capabilities. The NCCIC works closely with government at all levels and with the private sector to coordinate the integrated and unified response to cyber and communications incidents impacting homeland security.

Numerous DHS components, including US-CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Coordinating Center for Telecommunications (NCC), are collocated into the NCCIC. Also present in the NCCIC are other federal partners, such as the Department of Defense (DoD) and members of the law enforcement and intelligence communities. The NCCIC also physically collocates federal staff with private sector and non-governmental partners. Currently, representatives from the Information Technology and Communications sectors are located at the NCCIC. We are also finalizing steps to add representatives from the Banking and Finance sector, as well as the Multi-State Information Sharing and Analysis Center (MS-ISAC).

By leveraging the integrated operational capabilities of its member organizations, the NCCIC serves as an "always on" cyber incident response and management center, providing indications and warning of imminent incidents, and maintaining a national cyber "common operating picture." This facilitates situational awareness among all partner organizations, and also creates a repository of all vulnerability, intrusion, incident, and mitigation activities. The NCCIC also serves as a national point of integration for cyber expertise and collaboration, particularly when developing guidance to mitigate risks and resolve incidents. Finally, the unique and integrated nature of the NCCIC allows for a scalable and flexible coordination with all interagency and private sector staff during steady-state operations, in order to strengthen relationships and solidify procedures as well as effectively incorporate partners as needed during incidents.

Providing Technical Expertise to the Private Sector and Critical Infrastructure

DHS has significant cybersecurity capabilities, and we are using those capabilities to great effect as we work collaboratively with the private sector to protect the nation's CIKR. We engage with the private sector on a voluntary basis to provide onsite analysis, mitigation support, and

assessment assistance. Over the past year, we have repeatedly shown our ability to materially and expeditiously assist companies with cyber intrusion mitigation and incident response. We are able to do so through our trusted and close relationships with private sector companies as well as federal departments and agencies. Finally, our success in assisting the private sector is due in no small part to our dedication to properly and fully addressing privacy, civil rights and civil liberties in all that we do. Initiating technical assistance with a private company to provide them analysis and mitigation advice is a sensitive endeavor—one that requires trust and strict confidentiality. Within our analysis and warning mission space, DHS has a proven ability to provide that level of trust and confidence in the engagement. Our efforts are unique among federal agencies' capabilities in that DHS focuses on computer network defense and protection rather than law enforcement or intelligence functions. DHS engages precisely to mitigate the threat to the network to reduce future risks.

Our approach requires vigilance and a voluntary public/private partnership. Indeed, we are continuing to build our capabilities and our relationships; we must because the cyber threat trends only more sophisticated and more frequent.

Over the past year, we stood up the NCCIC and are adding staff to that center, both from existing DHS personnel and from partner organizations in the public and private sectors. More broadly, we are continuing to hire more cybersecurity professionals and are increasing training available to our employees. We have an operational National Cyber Incident Response Plan (NCIRP), and we continue to update and improve it with input from senior cybersecurity leaders. We will be releasing the NCIRP publicly in the coming weeks. We are executing within our current mission and authorities now: receiving and responding to substantial netflow data from our intrusion detection technologies deployed to our federal partners, and leveraging that data to provide early warnings and indicators across government and industry. With our people, processes and technology, we stand ready to execute the responsibilities of the future.

US-CERT provides remote and onsite response support and defense against malicious cyber activity for the Federal Executive Branch civilian networks. US-CERT also collaborates, provides remote and onsite response support and shares information with state and local government, critical infrastructure owners and operators, and international partners to address cyber threats and develop effective security responses.

In addition to specific mitigation work we conduct with individual companies and sectors, DHS looks at the interdependencies across critical infrastructure sectors for a holistic approach to providing our cyber expertise. For example, the electric, nuclear, water, transportation, and communications sectors support functions across all levels of government including federal, state, local, and tribal governments, and the private sector. Government bodies and organizations do not inherently produce these services and must rely on private sector organizations, just as other businesses and private citizens do. Therefore, an event impacting control systems has potential implications at all these levels, and could also have cascading effects upon all 18 sectors. For example, water and wastewater treatment, chemical, and transportation depend on the energy sector, and failure in one of these sectors could subsequently affect government and private sector operations.

NCCIC's operations are complemented in the arena of industrial control systems by ICS-CERT. The term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as energy, drinking water, emergency services, transportation, postal and shipping, and public health. Control systems security is particularly important because of the inherent interconnectedness of the CIKR sectors and their dependence on one another.

As such, assessing risk and effectively securing industrial control systems are vital to maintaining our nation's strategic interests, public safety, and economic well-being. A successful cyber attack on a control system could result in physical damage, loss of life, and cascading effects that could disrupt services. DHS recognizes that the protection and security of control systems is essential to the nation's overarching security and economy. In this context, as an example of many related initiatives and activities, DHS—in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), the Department of Energy, and DoD—has provided a forum for researchers, subject matter experts and practitioners dealing with cyber-physical systems security to assess the current state of the art, identify challenges, and provide input to developing strategies for addressing these challenges. Specific infrastructure sectors considered include energy, chemical, transportation, water and wastewater treatment, healthcare and public health, and commercial facilities. A 2010 published report of findings and recommendations is available upon request.

ICS-CERT provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.

A real-world threat emerged last year that significantly changed the landscape of targeted cyber attacks on industrial control systems. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware.

ICS-CERT analyzed the code and coordinated actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers. Our analysis quickly uncovered that sophisticated malware of this type potentially has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. In other words, this code can automatically enter a system, steal the formula for the product being manufactured, alter the ingredients being mixed in the product, and indicate to the operator and the operator's anti-virus software that everything is functioning normally.

To combat this threat, ICS-CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July 2010. To date, ICS-CERT has briefed dozens of government and industry organizations and released multiple advisories and updates to the industrial control

systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit. DHS provided the alerts in accordance with its responsible disclosure processes.

The purpose and function for responsible disclosure is to ensure that DHS executes its mission of mitigating risk to critical infrastructure, not necessarily to be the first to publish on a given threat. For example, ICS-CERT's purpose in conducting the Stuxnet analysis was to ensure that DHS understood the extent of the risks so that they could be mitigated. After conducting in-depth malware analysis and developing mitigation steps, we were able to release actionable information that benefited our private sector partners.

Looking ahead, the Department is concerned that attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems. Copies of the Stuxnet code, in various different iterations, have been publicly available for some time now. ICS-CERT and the NCCIC remain vigilant and continue analysis and mitigation efforts of any derivative malware.

ICS-CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, onsite incident response activities, and information sharing and partnerships.

Protecting Federal Civilian Government Networks

In addition to its support of private sector owners and operators of infrastructure, DHS also collaborates with its partners to increase the security of Federal Executive Branch civilian agency networks. The fundamental ways that DHS works to secure federal networks are by improving the ability of departments and agencies to defend their systems and by directly providing expertise and specific technology that detects, mitigates, and prevents malicious activity on these networks.

As part of the CNCI, DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. This initiative reduces the number of entry points for potential vulnerabilities into government networks and allows DHS to focus monitoring efforts on limited and known avenues through which Internet traffic must travel. DHS conducts onsite evaluations of agencies' progress toward implementing TIC goals.

In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity. The second phase of EINSTEIN, known as EINSTEIN 2 and developed in 2008 as part of the CNCI, incorporates intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian agency TIC locations and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, which are private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information. EINSTEIN 2 has now

been deployed at 15 of the 19 large departments and agencies who maintain their own TIC locations. Also, the four MTIPS providers currently provide service to seven additional federal agencies. In 2010, EINSTEIN 2 sensors registered 5.4 million "hits," an average of more than 450,000 hits per month or nearly 15,000 hits per day. A hit is an alert triggered by a predetermined intrusion detection signature that corresponds to a known threat. Each hit represents potential malicious activity for further assessment by US-CERT.

DHS is currently developing the third phase of the EINSTEIN system—an intrusion prevention capability which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems. In advance of this development, DHS, in coordination with the National Security Agency (NSA), conducted the CNCI Initiative 3 Exercise, which advanced the potential capabilities of the EINSTEIN system by demonstrating defensive technology, sharing near real-time threat information with DoD for enhanced situational awareness, and providing a platform upon which an oversight and compliance process can be implemented for the evolving set of EINSTEIN capabilities. The Department's Privacy Office and its Office for Civil Rights and Civil Liberties carefully reviewed the exercise concept of operations, and the Privacy Office worked with US-CERT to publicly release a detailed Privacy Impact Assessment evaluating the exercise. US-CERT also briefed the exercise to the cyber subcommittee of the independent DHS Data Privacy and Integrity Committee.

Beyond the TIC initiative and the EINSTEIN system, DHS, OMB, and the National Institute for Standards and Technology work cooperatively with agencies across the federal government to coordinate the protection of the nation's federal information systems through compliance with the Federal Information Security Management Act of 2002 (FISMA). US-CERT monitors EINSTEIN 2 sensors for intrusion activity and receives self-reported incident information from federal agencies. This information is reported to OMB for use in its FISMA oversight capacity. In 2010, DHS also began to administer oversight of the CyberScope system, which was developed by the Department of Justice. This system collects agency information regarding FISMA compliance and, as DHS, OMB and their agency partners move toward automated reporting, the system will enable real-time assessments of baseline security postures across individual agencies and the federal enterprise as a whole. This activity complements the development of reference architectures that DHS designs for federal agency stakeholders that are interested in implementing security solutions based on standards and best practices. DHS also works with the General Services Administration to create Blanket Purchase Agreements that address various security solutions for federal agencies.

The DHS Cybersecurity Workforce

As DHS continues to make progress on initiatives such as TIC and EINSTEIN, the Department is also mindful that the nation's cybersecurity challenge will not be solved by a single technology solution. Multiple innovative technical tools are necessary and indeed, technology alone is insufficient. The mission requires a larger cybersecurity professional workforce, governance structures for enhanced partnerships, more robust information sharing and identity protection, and increased cybersecurity awareness among the general public. Responsibility for these solutions is, and will remain, distributed across public and private sector partners.

DHS is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to our critical infrastructure and key resources. NCSD continues to hire cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in FY 2009 and nearly doubling that number again in FY 2010. NCSD currently has more than 230 cybersecurity professionals on board, with dozens more in the hiring pipeline.

Several initiatives are designed to increase the nation's number of highly qualified cybersecurity professionals. DHS and NSA co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which is to produce a growing number of professionals with information assurance expertise in various disciplines. DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the federal workforce. In December 2010, the Institute of Electrical and Electronics Engineers Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance (SwA) Curriculum Project. The MSwA program is the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. Finally, DHS co-sponsored the annual Colloquium for Information Systems Security Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 federal agencies and more than 200 SFS students.

The National Initiative for Cybersecurity Education (NICE) has the dual goals of a cyber-savvy citizenry and a cyber-capable workforce. Working with NIST, which is the overall interagency lead, DHS heads the NICE awareness elements and co-leads the training and professional development components with DoD and the Office of the Director of National Intelligence.

Interagency and Public-Private Coordination

Overcoming new cybersecurity challenges requires a coordinated and focused approach to better secure the nation's information and communications infrastructures. President Obama's *Cyberspace Policy Review* reaffirms cybersecurity's significance to the nation's economy and security. Establishment of a White House Cybersecurity Coordinator position solidified the priority the Administration places on improving cybersecurity.

No single agency controls cyberspace and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many government players have complementary roles—including DHS, the Intelligence Community, DoD, the Department of Justice, the Department of State, and other federal agencies—and they require coordination and leadership to ensure effective and efficient execution of our collective cyber missions. The creation of a senior-level cyber position within the White House ensures coordination and collaboration across government agencies.

DHS works closely with its federal, state and local partners to protect government cyber networks. In September 2010, DHS and DoD signed a memorandum of agreement that aligns

and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a National Security Agency support team to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to the National Security Agency.

In November 2010, the MS-ISAC opened its Cyber Security Operations Center, a 24-hour watch and warning facility, which will both enhance situational awareness at the state and local level for the NCCIC and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments. An MS-ISAC analyst/liaison is collocated in the NCCIC.

Private industry owns and operates the vast majority of the nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, and DHS has initiated several pilot programs to promote public-private sector collaboration. In its engagement with the private sector, DHS recognizes the need to avoid technology prescription and to support innovation that enhances critical infrastructure cybersecurity. DHS, through the National Infrastructure Protection Plan partnership framework, has many years of experience in private sector collaboration, leveraging our relationships in both the physical and cybersecurity protection areas. Within current legal authorities, DHS engages with the private sector on a voluntary basis. We stand by to assist our private sector partners upon their request, and thus far have been able to do so successfully due to our technical capabilities, existing private sector relationships, and expertise in matters relating to privacy and civil rights and civil liberties.

In February 2010, DHS, DoD, and the Financial Services Information Sharing and Analysis Center (FS-ISAC) launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information. Based on lessons learned from the pilot, DHS is developing comprehensive information-sharing and incident response coordination processes with CIKR sectors, leveraging capabilities from within DHS and across the response community, through the NCCIC.

In June 2010, DHS implemented the Cybersecurity Partner Local Access Plan, which allows security-cleared owners and operators of CIKR, as well as state technology officials and law enforcement officials, to access secret-level cybersecurity information and video teleconference calls via state and local fusion centers. In November 2010, DHS signed an agreement with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full-time IT-ISAC analyst and liaison to DHS at the NCCIC, part of the ongoing effort to collocate private sector representatives alongside federal and state government counterparts. The IT-ISAC consists of information technology stakeholders from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

In July 2010, DHS worked extensively with the White House on the publication of a draft National Strategy for Trusted Identities in Cyberspace, which seeks to secure the digital identities of individuals, organizations, services and devices during online transactions, as well as the infrastructure supporting the transaction. This fulfills one of the near-term action items of the President's *Cyberspace Policy Review*. The strategy is based on public-private partnerships

and supports the protection of privacy, and civil rights and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction. Its implementation will be led by the Department of Commerce.

In December 2010, DHS and NIST signed a Memorandum of Understanding with the Financial Services Sector Coordinating Council. The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our nation's critical infrastructures. This agreement will accelerate the deployment of network test beds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures.

While considerable activity is focused on public and private sector critical infrastructure protection, DHS is committed to developing innovative ways to enhance the general public's awareness about the importance of safeguarding America's computer systems and networks from attacks. Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cybersecurity Awareness Month. In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge, which called on the general public and private sector companies to develop creative and innovative ways to enhance cybersecurity awareness. In July 2010, seven of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals helped inform the development of the National Cybersecurity Awareness Campaign, *Stop. Think. Connect.*, which DHS launched in conjunction with private sector partners during the October 2010 National Cybersecurity Awareness Month. *Stop. Think. Connect.*, a message developed with the private sector, has evolved into an ongoing national public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's *Cyberspace Policy Review*, which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely. The program is part of the NIST National Initiative for Cyber Education (NICE).

Throughout its public and private sector activities, DHS is committed to supporting the public's privacy, civil rights and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all of its cybersecurity programs and initiatives from the outset. To support this, DHS established an Oversight and Compliance Officer within NPPD, and key cybersecurity personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities. In an effort to increase transparency, DHS also publishes privacy impact assessments on its website, www.dhs.gov, for all of its cybersecurity systems.

Conclusion

Set within an environment characterized by a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a national one requiring collaboration across the homeland security enterprise. The Department of Homeland Security is committed to creating a safe, secure and resilient cyber environment while promoting

cybersecurity knowledge and innovation. We must continue to secure today's infrastructure as we prepare for tomorrow's challenges and opportunities. It is important to recognize that we do not undertake cybersecurity for the sake of security itself, but rather to ensure that government, business and critical societal functions can continue to use the information technology and communications infrastructure on which they depend.

Within our current legal authorities, DHS continues to engage and collaborate with partners in the private and public sectors. We are deploying intrusion detection and prevention technologies across the federal enterprise, aiding departments and agencies in securing their networks, and providing analysis, vulnerability, and mitigation assistance to private sector CIKR partners. Our continued dedication to privacy, civil rights and civil liberties ensures a positive, sustainable model for cybersecurity engagement in the future. Finally, we work closely with our interagency partners in law enforcement and intelligence, providing the full complement of federal capabilities in preparation for, and in response to, significant cyber incidents.

Chairman Lungren, Vice Chairman Walberg, Ranking Member Clarke, and distinguished Members of the Subcommittee, let me end by reiterating that I look forward to exploring opportunities to advance this mission in collaboration with the Subcommittee and my colleagues in the public and private sectors. Thank you again for this opportunity to testify. I would be happy to answer your questions.