

Statement for the Record
of
Seán P. McGurk
Director, National Cybersecurity and Communications Integration Center
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
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Washington, DC

April 15, 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. Specifically, I will discuss the Department's cybersecurity mission as it relates to critical infrastructure and our coordination of this mission with the private sector.

Deputy Under Secretary Philip Reitinger recently testified before this Subcommittee, and I would like to reiterate the Department's desire to work more with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on in our 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 faces 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 sharing of information. As bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We face threats that could significantly compromise the accessibility and reliability of our information infrastructure.

Malicious actors in cyberspace, including nation states, terrorist networks, organized criminal groups, and individuals located here in the United States, 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, 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. 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 across the public and private sectors.

We need to support the efforts of our private sector partners to secure themselves against malicious activity in cyberspace. Collaboratively, public and private sector partners must use our knowledge of information technology 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.

Cybersecurity Mission

No single technology—or single government entity—alone can overcome the cybersecurity challenges our nation faces. Consequently, the public and private sectors must work collaboratively. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort among the private sector, including critical infrastructure owners and operators, and the extensive expertise that lies across coordinated government entities. In addition to leading the effort to secure Federal Executive Branch civilian departments and agencies' unclassified networks, the National Protection and Programs Directorate (NPPD) within DHS is responsible for the following key cybersecurity missions:

- 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.

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 continue to evolve as 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 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. It also houses the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber and communications watch and warning center. 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 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. Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace. Although DHS leads significant cybersecurity mission activities in the public sector, I will focus the rest of my testimony on private sector coordination.

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, are collocated in 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 and the Multi-State Information Sharing and Analysis Center are located on the NCCIC watch floor. We are also finalizing steps to add representatives from the Banking and Finance Sector, as well as the Energy Sector .

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 reported 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.

NCSD collaborates with private sector stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, incident response assistance, and exercise opportunities for 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 (NCIRP). The NCIRP 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 NCIRP 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 NCCIC and the federal government’s full suite of cybersecurity response capabilities.

Providing Technical Operational Expertise to the Private Sector

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 demonstrated 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 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 civilian computer network defense and protection rather than law enforcement, military, or intelligence functions. DHS engages to mitigate the threat to the network to reduce future risks.

Our approach requires vigilance and a voluntary public/private partnership. We are continuing to build our capabilities and relationships because the cyber threat trends are more sophisticated and frequent.

Over the past year, we established 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 increasing training availability to our employees. The NCIRP is operational, and we continue to update and improve it with input from senior cybersecurity leaders. We will be releasing the NCIRP publicly in the near future. 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.

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 sectors depend on the Energy Sector, and failure in one of these sectors could subsequently affect government and private sector operations.

US-CERT also collaborates, provides remote and onsite response support, and shares information with federal, state and local governments; critical infrastructure owners and operators; and international partners to address cyber threats and develop effective security responses.

DHS provides onsite and remote incident response assistance to its public and private sector partners. Upon notification of a cyber incident, ICS-CERT and/or US-CERT can perform a preliminary diagnosis to determine the extent of the compromise. At the partner's request and when appropriate, either ICS-CERT or US-CERT can deploy a team to meet with the affected organization to review network topology, identify infected systems, create image files of hard drives for analysis, and collect other data as needed to perform thorough follow-on analysis. Both ICS-CERT and US-CERT can provide mitigation strategies, advise asset owners and

operators on their efforts to restore service, and provide recommendations for improving overall network and control systems security.

An incident in early 2010 illustrates the incident response support that DHS provides. In this case, an employee of a company had attended an industry event and used an instructor's flash drive to download presentation materials to the company's laptop. The flash drive was infected with the Mariposa botnet, unbeknownst to the event organizer. When the employee returned to the work location and used the laptop, the virus quickly spread to nearly 100 systems. US-CERT and ICS-CERT had already been tracking a trend of removable media involved in malware infections, and, on request, deployed a team to the company's location to help diagnose the malware and identify those infected systems.

The team spent two days with the company reviewing the incident details, network topology, and the company's control systems architecture to identify systems of interest. The company was ultimately able to leverage all of the information to contain the infection and remove the malware from the infected systems. ICS-CERT and US-CERT provided follow-on reporting, mitigation measures, and access to additional resources through the US-CERT secure portal.

US-CERT'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, 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.

An additional 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, our goal is to balance the need for public information sharing while protecting 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.

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 has sole responsibility for securing cyberspace, and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many government players have complementary roles as well as unique capabilities—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.

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. For example, the Office of Infrastructure Protection and the National Cyber Security Division partnered with the chemical industry to publish the *Roadmap to Secure Industrial Control Systems in the Chemical Sector* in 2009, available at www.us-cert.gov. To meet the first set of milestones set forth in this 10-year plan, industry, in partnership with DHS, developed a suite of control systems security awareness materials that will be shared widely within the Chemical Sector this summer.

DHS engages with the private sector on a voluntary basis in accordance with our responsibilities under the Homeland Security Act. 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 major urban area 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. The final strategy is set to be released in the near

future, fulfilling 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 September 2010, Secretary Napolitano and Secretary Gates co-signed a Memorandum of Agreement between DHS and DoD regarding cybersecurity. The MOA established a Joint Coordination Element (JCE) led by a DHS senior official at DoD's National Security Agency. The intent of the MOA was to enable DHS and DoD to leverage each other's capabilities, and more readily share cybersecurity information on significant cyber incidents. The JCE has been in place and building to fully operational capability since October 2010.

In December 2010, the DHS Science and Technology Directorate 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.

Collaborative Risk Management Forums

The increased pace of collaborative cybersecurity operations between DHS and the private sector is due, in part, to standing public-private forums that support ongoing process improvements across the partnership. A few of these forums -- the Cross-Sector Cyber Security Working Group, the IT CIKR Sector, and the Industrial Control Systems Joint Working Group -- meet under the auspices of the Critical Infrastructure Partnership Advisory Council and conduct their activities consistent with the National Infrastructure Protection Plan (NIPP) partnership framework.

The Cross-Sector Cyber Security Working Group was established 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 and planning documents including the NCIRP, the President's *Cyberspace Policy Review*, and the *National Strategy for Trusted Identities in Cyberspace*.

The IT CIKR Sector security partnership is comprised of DHS as the IT Sector Specific Agency, public sector partners in the IT Government Coordination Council, and private sector partners in the IT Sector Coordinating Council. This partnership forms to execute the IT Sector's risk management framework: to identify and prioritize risks to IT Sector critical functions, to develop and implement corresponding risk management strategies, and to report on progress of risk management activities and adjustments to the IT Sector's risk profile. IT Sector public-private partners worked collaboratively to produce the 2009 IT Sector Baseline Risk Assessment (ITSRA), prioritizing risks to the sector's critical functions, and have subsequently been working to finalize corresponding risk management strategies outlining a portfolio of sector risk management activities to reduce the evaluated risks from the ITSRA across the functions.

Progress reporting on implementation of these risk management strategies will be provided in the IT Sector Annual Report (as required by the NIPP).

In partnership with the Department of Energy, which is the Sector Specific Agency responsible for the Energy Sector under the NIPP, the Industrial Control Systems Joint Working Group provides a vehicle for stakeholders to communicate and partner across all critical infrastructure sectors to better secure industrial control systems and manage risk. The Industrial Control Systems Joint Working Group is a representative group comprising owners and operators, international stakeholders, government, academia, system integrators, and the vendor community. The purpose of the ICSJWG is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, deployment and secure operations of industrial control systems. Based on public and private sector partner input, CSSP uses the Industrial Control Systems Joint Working Group to inform its mission activities and deliver needed products and services.

As you are aware, cybersecurity training is essential to increasing awareness of threats and the ability to combat them. To that end, CSSP conducts multi-tiered training through web-based and instructor-led classes across the country. In addition, a week-long training course is conducted at CSSP's state-of-the-art advanced training facility at the Idaho National Laboratory to provide hands-on instruction and demonstration. This training course includes a red team/blue team exercise in which the blue team attempts to defend a functional mockup control system while the red team attempts to penetrate the network and disrupt operations. The positive response to this week-long course has been overwhelming, and the classes are filled within a few days of announcement. To date, more than 16,000 public and private sector professionals have participated in some form of CSSP training through classroom venues and web-based instruction.

CSSP also provides leadership and guidance on efforts related to the development of cybersecurity standards for industrial control systems. CSSP uses these industry standards in a variety of products and tools to achieve its mission.

First, CSSP uses and promotes the requirements of multiple federal, commercial and international standards in its Cyber Security Evaluation Tool (CSET), which has been requested by and distributed to hundreds of asset owners across each of the 18 CIKR sectors. Tool users are evaluated against these standards based on answers to a series of standard-specific questions. CSET is also used by CSSP assessment teams to train and bolster an asset owner's control system and cybersecurity posture in onsite assessments. In fiscal year 2010, the program conducted more than 50 onsite assessments in 15 different states and two U.S. territories, including several remote locations where the control systems represent potential single points of failure for the community. The program is planning for 75 onsite assessments in fiscal year 2011.

Second, CSSP developed the *Catalog of Control Systems Security: Recommendations for Standards Developers*, which brings together pertinent elements from the most comprehensive and current standards related to control systems. This tool is designed as a superset of control

systems cybersecurity requirements and is available in the CSET and on the website for standards developers and asset owners.

Lastly, the CSSP provides resources, including time and expertise, to standards development organizations including NIST, the International Society of Automation, and the American Public Transportation Association. Experts provide content, participate in topic discussions, and review text being considered by the standards body.

The General Public

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, 7 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.*, 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.

DHS is committed to safeguarding 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 broad collaboration. DHS 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. Cybersecurity is critical to ensure that government, business and the public can continue to use the information technology and communications infrastructure on which they depend.

DHS continues to engage, collaborate and provide analysis, vulnerability, and mitigation assistance to its private sector CIKR partners. Our continued dedication to privacy and 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, military, 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 conclude 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.