Statement for the Record

Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
September 14, 2009

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for inviting me to appear before you today to discuss the work of the Department of Homeland Security (DHS) to improve the Nation's cybersecurity. The Committee's topic, "Cyber Attacks: Protecting Industry Against Growing Threats," is quite possibly the most critical and complicated matter on the Nation's cybersecurity agenda. The security of private sector information, systems, and networks is essential for the activities of today's businesses and consumers. And, since much of our nation's critical infrastructure is in industry hands, ensuring the security of private-sector cyber resources is a vital part of the Nation's overall cybersecurity.

The President has developed a coordinated approach to cybersecurity which elevates cybersecurity in the White House. This approach includes the appointment of a Chief Technology Officer, located in the Office of Science and Technology Policy, a Chief Information Officer in the Office of Management and Budget, and the pending appointment of a cybersecurity policy official in the White House. This team provides an effective means for coordination and collaboration – across the Federal government and with the private sector - underscoring the high priority the administration places on securing cyber space. At DHS we

work closely on all cybersecurity matters with this leadership team and the rest of the federal agencies to ensure a coherent, coordinated approach with the private sector.

DHS has both broad and specific responsibilities for cybersecurity. Secretary Napolitano has designated me as the focal point and coordinator for DHS's cybersecurity responsibilities, both in my role as the Deputy Under Secretary of the National Protection and Programs Directorate (NPPD) and as the Director of the National Cyber Security Center. Specifically, DHS has responsibility for enabling the Federal civilian agencies to secure their information, systems, and networks. Additionally, we lead the Federal Executive Branch's work with America's private sector to secure the communications and information infrastructure critical to our economy and way of life. This infrastructure, sometimes referred to as the dot com domain, is largely owned and operated by the private sector. As a result, DHS and the broader Federal Government must rely on our private sector partners as we work to ensure that resiliency, security, privacy, and other critical protections are built into our evolving infrastructures.

While today's hearing focuses on our work with the private sector, we are also very concerned with protecting the dot gov domain. I look forward to talking with Committee about those activities in the near future. And, as the testimony of Assistant Director Merritt of the United States Secret Service illustrates, DHS has other missions and capabilities in the cybersecurity domain. In all this work, DHS requires and receives strong support from the White House, Congress, and the Federal agencies that own and operate their own systems or are the subject matter experts and regulatory contacts for specific parts of the private sector.

My current activities reflect three top priorities. The first priority is building capacity – primarily human, but also technical capacity – within DHS. With excellent support from the Administration and Congress, we have grown aggressively over the past several years to build a world-class, sustainable cybersecurity workforce that can successfully address this complex and growing challenge. Much of this workforce is focused on our mission to secure the dot gov (Federal civilian agency) domain. This includes leading a number of activities under the Comprehensive National Cybersecurity Initiative and the Administration's Cyberspace Policy Review. As the Committee knows, Federal information technology (IT) systems are under constant attack—via the Internet and other means—from individuals and groups that seek to disrupt, deny access to, degrade, or destroy those systems and the data contained on them. A comprehensive Federal network defense entails: situational awareness of the state of networks; an early warning capability; near real-time and automatic identification of malicious activity; and the ability to deflect or disable malicious activity before harm is done. DHS, through the National Cyber Security Division, is developing a system-of-systems approach that encompasses the people, activities, processes, and technologies needed to fulfill its cybersecurity mission. DHS is implementing the Trusted Internet Connection initiative, a multi-faceted program for improving the Executive Branch's cybersecurity posture by reducing the number of external internet connections. Further, we are leading the deployment of the EINSTEIN program, which is creating intrusion detection and prevention capabilities on Federal networks. In this, as in all our work, enhancing the privacy and civil liberties of the American public is at the core of our strategy and approach.

My second priority is building partnerships with key stakeholders inside and outside government, including strengthening our working relationships with the private sector on all levels. I will briefly highlight specific examples of our work with the private sector, they are as follows:

Incident Response

The President's Cybersecurity Policy Review calls for "a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident." DHS has the lead for this initiative; we are managing a working group comprised of representatives from the private and governmental (Federal, State, and local) sectors to develop a National Cyber Incident Response Plan (NCIRP). This will produce a clear delineation of roles and responsibilities in case of a major cyber incident, and it will update the Cyber Incident Response Annex to the National Response Framework created under Homeland Security Presidential Directive 5. Most importantly, we have launched this process with the private sector integrated from the very start to establish an actionable response framework that will allow us to respond to a cyber incident as one Nation, not just as one government. In concert with the NCIRP, we are designing and developing a DHS-managed alert and warning system for cyber-related incidents as well as updating concepts of operations, standard operating procedures, and playbooks.

A key part of successful incident response is the ability to coordinate operations across multiple organizations. In this regard, DHS is building an integrated cybersecurity and communications

watch floor that will collocate the capabilities of various DHS cybersecurity and communications-related response organizations. This joint watch floor, which will be operational before the end of 2009, will also provide additional capacity for State and local government and private sector participants to be physically and virtually present at the front lines of the national response, strengthening capability and building trust though operational activity. This consolidation of capability has been recommended by the President's National Security Telecommunications Advisory Committee (NSTAC) and by other expert groups.

We expect to test the NCIRP early next year and exercise it, with substantial participation from the private sector, during the Cyber Storm III exercise in September 2010.

Advisory Groups

Enormous cybersecurity expertise resides in the private sector, in the information and communications technology industry, and within the critical infrastructure sectors. DHS sponsors a variety of advisory groups pertinent to cybersecurity issues. These include two Presidential advisory committees -- the NSTAC and the National Infrastructure Advisory Council -- and a variety of DHS-specific committees and working groups under the framework of the Critical Infrastructure Partnership Advisory Council.

The Cross-Sector Cyber Security Working Group, for example, is a DHS-specific committee working to facilitate the bi-directional sharing of operational cybersecurity information within and across critical infrastructure sectors and government agencies, including indications and

warnings in advance of incidents. In addition, the Information Technology Sector Coordination Council and DHS co-published the IT Sector Baseline Risk Assessment in August 2009, providing the basis for identifying IT risks to national and economic security, public health and safety, government services, and the operation of other critical infrastructure. It is an all-hazards risk assessment that provides an evaluation of the IT sector's threats, vulnerabilities, and consequences and informs the development of strategies to mitigate sector-wide risks. This baseline assessment is an example of how government and industry can collaboratively create a basis for making more informed decisions about security.

There are finite resources in both government and industry to address ever-changing and emerging requirements; we must collectively make the most efficient use of our energies. In order to ensure that DHS is working most efficiently, we are reviewing the roles and responsibilities of the various advisory bodies in order to determine how to most effectively utilize the time and commitment of the private sector in this complex arena and ensure that the Government is best able to implement their recommendations.

Information Sharing

As suggested above, the sharing of cybersecurity information, indications, and warnings between government and the private sector can prevent or mitigate the consequences of attacks. For example, when DHS' 24/7 watch and warning center, the United States Computer Emergency Readiness Team (US-CERT), becomes aware of potential or ongoing efforts to compromise government and private sector systems, it shares this information with federal and industry

partners. This information sharing helps prevent or minimize disruptions to critical information infrastructures and protect the economy, government services, and the national security of the United States. US-CERT has released more than 40 alerts and products during the first eight months of 2009. The products are used by many public and private sector entities, domestically and internationally, to increase the security of their networks and data.

US-CERT is taking steps to improve its capabilities in this area. For example, US-CERT recently developed the Joint Agency Cyber Knowledge Exchange (JACKE), a secure conference call/meeting among cyber and IT analysts and engineers, to improve situational awareness and recommend actions for Federal agency security operation centers. Fifteen agencies are participating, and our next step is to expand participation in JACKE to include all 26 major departments and agencies. We believe this effort will produce or influence products that will be helpful to the private sector as well.

Further, earlier this year, DHS hosted an Industry Day to highlight the need for private industry to become more involved in developing comprehensive, game-changing, innovative solutions that improve and expand upon current capabilities. As a follow-up, DHS released a request for information to the private sector to identify prospective private sector technical, end-to-end solutions for protecting the Federal cyber domain.

Cybersecurity Awareness

In October, we will mark the sixth annual Cybersecurity Awareness Month. This year's focus is on promoting shared responsibility for cybersecurity among all stakeholders, including the creation of a culture of cybersecurity in organizations. As in past years, DHS is working with stakeholder organizations such as the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center to expand our reach into to the private sector both on a nationwide and state-by-state basis.

Cyber Crime

I want to touch briefly on cyber crime, given the composition of the rest of today's panel. For most private sector organizations, and especially for small businesses, attacks by cyber criminals trying to steal businesses' financial resources are the greatest and most proximate cybersecurity concern. Cyber criminals have moved far beyond the mere disruption and hacker reputation building activities of a bygone era—cyber criminals now look for money and value. There are many simple steps that businesses can and should take to protect themselves. Securing the entrances of one's factory or store is second nature to any business owner and so cyber security protections must become. A recent public report from Verizon's business risk team estimated that 87 percent of data breaches could be avoided by simple to intermediate preventative measures. And yet many small businesses do not keep their virus protections or firewalls up to date. Simple hygiene of this type can go a long way to preventing cyber crimes. US-CERT provides valuable tips and guidance at www.us-cert.gov, as well as links to other resources.

Finally, my third priority looks to the long term, we are anticipating and driving change in the public-private cyber ecosystem. For example, we intend to:

- Work with our partners across the government and private sector to ensure that: incentives and requirements for security align with national and homeland security needs; metrics enable distributed actors to make judgments about security based on data; and future architectures meet national needs for security and resiliency, including in the areas of software assurance, supply chain protection, and risk assessment;
- Build interoperability in communications and information for confidentiality, integrity, and availability;
- Work with partners in government and critical infrastructures to create and implement a vision and system that will enable the authentication of people, processes, and devices, protecting privacy by design and mitigating major categories of threats and threat actors; and
- Build cybersecurity both as a profession and as a core element of other professions, equipping the next generation of leaders and operators to succeed.

Conclusion

The Nation's critical networks and systems are vulnerable to a persistent, evolving and sophisticated cyber threats. DHS, in conjunction with its public and private sector partners, is at the vanguard of the efforts to secure those networks and systems. With the support and leadership of the White House, Secretary Napolitano has focused the Department so that cybersecurity will receive the high-level attention it merits.

We cannot solely pay attention to today's challenges. The dynamic cybersecurity environment demands constant innovation, and we are collaborating with others to anticipate future cybersecurity challenges so that we can outpace our adversaries. DHS is building a holistic, comprehensive, long-term cybersecurity vision and strategy that relies on a collaborative approach. A key component of that effort is building a world-class cyber workforce to meet the demands of both today and the future. We must also build awareness and understanding of cybersecurity issues among the public. While DHS has already built a robust public-private cyber partnership, we expect that partnership to continue to mature. There is much more work to be done and we must all work together if we are to accomplish the mission. I look forward to working with this Committee in that effort.

Thank you, and I would be pleased to answer any questions.