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 the Judiciary
Subcommittee on Terrorism and Homeland Security

Chairman Cardin, Ranking Member Kyl, and members of the Subcommittee, 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. Criminals and other adversaries attack critical U.S. systems every day, stealing valuable information, diverting funds to support criminal or terrorist activities, and compromising the online identities of Americans. The need to effectively prevent, protect against, and respond to these attacks is critical to the Nation's economic and national security, and both the public and private sectors have significant efforts underway that work toward preventing and disrupting cyber attacks against these assets.

Secretary Napolitano has designated me as the lead for DHS' broad set of 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. DHS is charged with protecting and defending both the federal government's civilian information systems and networks as well as collaborating with the private sector to ensure the resilience of privately owned infrastructure.

To secure the federal executive branch's civilian networks and systems, DHS collaborates with its interagency partners. Currently, DHS is upgrading the federal government's capabilities to secure and defend against threats from individuals or organizations in cyberspace. In particular, the Department is focused on network defense activities geared toward defeating attacks from sophisticated high-level threat actors, that is, those who can potentially damage, cripple, and exploit these networks and systems. We are also working with federal civilian agencies to better secure their information systems and networks.

DHS also leads the federal government's work with the private sector to secure the Nation's critical communications and information technology infrastructure. This infrastructure—including the control systems that support the operations of electrical grids, manufacturing, health care, and banking—is largely owned and operated by the private sector. DHS collaborates with our private sector partners to ensure that resiliency, security, privacy, and other critical protections are built into these continually evolving infrastructures.

DHS has other cybersecurity mission areas beyond those of protecting federal and private sector networks and infrastructure. Specifically, the United States Secret Service investigates violations of U.S. laws relating to financial crimes and computer fraud and abuse. U.S. Immigration and Customs Enforcement's Cyber Crimes Center leads many trans-border criminal investigations into Internet-related crimes. And DHS' Science and Technology Directorate manages a full cybersecurity Research and Development lifecycle portfolio. In all this work, DHS has strong support from the White House, Congress, and our federal interagency partners, for our efforts to secure the systems, networks, and information on which we all rely in a manner

that enhances individual privacy and civil liberties, ensures that we remain true to our national values and operate within existing legal frameworks.

Given the interests of this Committee, I will turn my focus to two particular matters: our efforts to prevent and disrupt cyber attacks, and legal and privacy issues relating to cybersecurity.

Preventing and Disrupting Cyber Attacks

The Nation's electronic information infrastructure is vital to the functioning of government as well as to maintaining the Nation's economy and national security. This infrastructure comes under attack from a variety of sources, ranging from novice hackers to sophisticated groups that seek to gain or deny access to, disrupt, degrade, or destroy the systems and the data contained therein. As more of our critical infrastructure is connected to the Internet, malicious cyber activity will only increase and become more sophisticated and targeted, creating ever-greater potential for more severe consequences.

President Obama outlined the Administration's approach to cybersecurity in a public address in May. Under this plan, the Department of Homeland Security is leading efforts to secure federal executive branch civilian government networks. The Department, acting in its network defense capacity, treats sophisticated attacks from high-level threat actors as a key priority—we also work with critical infrastructure sectors to increase their cybersecurity. We maintain close ties with our intelligence and law enforcement partners, and we work to ensure that the overall level of preparedness is increasing in response to specific known and expected types of attacks from

any source. I would like to discuss four areas of work that support DHS' government and private sector cybersecurity missions. The first, cybersecurity protection, focuses primarily on government systems while the other three—incident response, collaboration and information sharing, and public awareness—focus on public/private partnership.

Cybersecurity Protection

The use of advanced technologies helps DHS improve its cybersecurity support to federal departments and agencies—for example, DHS' National Cybersecurity Division's (NCSD) within NPPD utilizes existing and currently deployed network flow monitoring and intrusion detection capabilities. DHS created the National Cybersecurity Protection Program to support the National Cybersecurity Protection System, operationally known as EINSTEIN. There are two versions of EINSTEIN at this time: EINSTEIN 1, a network flow monitoring system, and EINSTEIN 2, an intrusion detection system. In the future, DHS envisions deploying EINSTEIN 3, an intrusion prevention system, for federal executive branch civilian networks and systems. This more robust version of EINSTEIN would provide the federal government with an improved early warning and an enhanced situational awareness; the ability to automatically detect malicious activity; and the capability to prevent malicious intrusions before harm is done. In addition to this specific program, DHS has a variety of other initiatives under way to enhance the cybersecurity of civilian federal executive branch agencies and elements of the critical infrastructure. These include:

- Consolidating agencies' external Internet connections to reduce the number of entry points for potential outside threats;
- Developing a supply chain risk management framework to address security threats and vulnerabilities that could be introduced into hardware and software acquired by federal agencies;
- Establishing the Industrial Control Systems Cyber Emergency Response Team facility, which just opened earlier this month, to synchronize incident response activities related to attacks on control systems operating the Nation's critical infrastructure. It provides onsite forensic investigations and situational awareness in the form of actionable information, coordinates the responsible disclosure of vulnerabilities and mitigation solutions, and shares vulnerability information and threat analysis;
- Initiating an information-sharing pilot working with the Financial Services Information Sharing and Analysis Center to enhance threat information sharing with the financial services sector. The pilot is based on the good work that the Department of Defense has done with the Defense Industrial Base sector to increase actionable bi-directional information sharing.

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 and is managing an interagency, state and local government, and private sector working group to develop a National Cyber Incident Response

Plan (NCIRP). This work will produce a clear delineation of roles and responsibilities in case of a major cyber incident and 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, so that the end result will be an actionable response framework that will allow us to address a cyber incident as one Nation. In concert with the NCIRP, we are in the process of 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 recently launched the National Cybersecurity and Communication Integration Center (NCCIC). As recommended by the President's National Security Telecommunications Advisory Committee and by other expert groups, the NCCIC co-locates the capabilities of various DHS cybersecurity and communications-related response organizations. Secretary Napolitano stated at the launch that the NCCIC will "serve as the central repository for cyber threat and incident reporting and provide improved operational situational awareness across the federal government, particularly across the civilian side of the federal government, as well as with the private sector." As it matures, we will incorporate additional capacity for state and local government participation onto the NCCIC operations floor. The NCCIC strengthens existing capabilities, and will continue to build trust by bringing together organizations whose common purpose is to protect shared cyber infrastructure. Early next year, we expect to exercise the NCCIC's operations, as well as the new response procedures defined in the NCIRP; further, during the Cyber Storm III exercise in September 2010, we will test these operations with substantial participation from the private sector.

Collaboration and Information Sharing

Effective collaboration across government and industry has the potential to mitigate and even prevent a cyber attack. For example, when DHS's United States Computer Emergency Readiness Team (US-CERT) becomes aware of potential or occurring efforts to compromise government and/or private sector systems, it works with federal and industry partners to prevent or minimize disruptions to critical information infrastructures and protect the economy, government services, and the Nation's security. During Fiscal Year 2009, US-CERT produced more than 130 products to increase network and data security of public and private—both domestic and international—entities; sent over 30 alerts to the Government Forum of Incident Response and Security Teams (GFIRST), and posted more than 290 alerts to the US-CERT public-facing website.

As US-CERT upgrades its defensive technological and analytical capabilities, including EINSTEIN, the timeliness and quality of its products will improve. In addition to sending information to key stakeholders and the public, US-CERT is working to improve its operational collaboration with other federal agency responders. Last year, DHS established the Joint Agency Cyber Knowledge Exchange (JACKE), an interagency forum of federal agency cybersecurity incident responders. The JACKE provides a venue for customer feedback to US-CERT and recommendations to improve the practices of federal security operation centers. Fifteen agencies are participating, and the next step is to expand participation to include all 26 major departments and agencies. We believe efforts like JACKE will help US-CERT better understand the views of

its customers, thereby improving its products and services. This process will also better inform the products we share with the private sector and the public.

Finally, 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 our current capabilities. As a follow-up, DHS released a classified request for information to the private sector to identify prospective private sector technical, end-to-end solutions for protecting the federal cyber domain.

Public Awareness

As stated in the President's Cyberspace Policy Review, *"People cannot value security without first understanding how much is at risk. Therefore, the Federal government should initiate a national public awareness and education campaign."* In that spirit, DHS reached out to the public broadly in October, during the sixth annual Cybersecurity Awareness Month, which focused this year on shared responsibility. During the month, Secretary Napolitano delivered three public speeches on cybersecurity and participated in several other outreach efforts, including meetings in Silicon Valley with industry leaders and two public web chats broadcast on www.dhs.gov. In support of these efforts, other DHS personnel delivered nearly 60 cybersecurity speeches in October, promoting shared responsibility for cybersecurity among all stakeholders, including the creation of a culture of cybersecurity in organizations. As in past years, DHS worked with stakeholder organizations such as the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center to expand our reach into the private

sector. We will continue this important work with stakeholders and partners in the months ahead.

Legal and Privacy Issues

Efforts to secure cyberspace are accompanied by complex, interrelated, and international legal and privacy issues. Let me turn first to general legal issues, and then more specifically to privacy. As the President's Cyberspace Policy Review notes:

"Law applicable to information and communications networks is a complex patchwork of Constitutional, domestic, foreign, and international laws that shapes viable policy options…As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests…Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork …or the applications of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles."

DHS works closely with DOJ and other agencies to resolve specific legal issues around particular activities. For example, as the Subcommittee is aware, the DOJ Office of Legal Counsel has issued opinions regarding the EINSTEIN 2 program and affirming its compliance with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, 18 U.S.C. § 270(a)(1), the pen register, and trap and trace provisions of chapter 206 of title 18, United States Code.[1] We will continue to work closely with DOJ to proactively address these important legal issues as we improve our defensive cybersecurity capabilities.

In this regard, the Comprehensive National Cybersecurity Initiative (CNCI) effort operates under executive guidance that all actions pursuant to this initiative will be implemented in a manner that ensures protection of privacy rights and other legal rights of Americans. The Secretary of Homeland Security is the lead official for the national effort to protect, defend, and reduce vulnerabilities of federal executive branch civilian systems. Accordingly, the specific privacy provisions[2] of section 222 of the Homeland Security Act apply to all DHS cybersecurity and CNCI activities.

Compliance with privacy statutes is critical, but even more can be done: increased cybersecurity creates an opportunity to enhance privacy and civil liberties. Whether it is by lowering the incidence of identity theft through stronger authentication regimes, or by protecting anonymity

[1] *See* Memorandum Opinion for an Associate Deputy Attorney General, Legality Of Intrusion-Detection System To Protect Unclassified Computer Networks In The Executive Branch (August 14, 2009); Memorandum Opinion for the Counsel to the President, Legal Issues Relating To The Testing, Use, And Deployment Of An Intrusion-Detection System (Einstein 2.0) To Protect Unclassified Computer Networks In The Executive Branch (January 9, 2009), both available at http://www.justice.gov/olc/allopinions.htm.

[2] In particular, that section charges the Department's Chief Privacy Officer with "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."

on government websites where free speech or privacy considerations are predominant, the U.S. government must lead the way, in cooperation with our state and local partners and the private sector.

Accordingly, DHS and its partners have taken decisive steps as we add, upgrade, and build upon existing defensive cybersecurity capabilities. DHS has, and will continue to incorporate privacy rights and civil liberties protections into the operating procedures and the architectural engineering development and deployment schedule for each iteration of EINSTEIN. As an added layer of protection, DHS has created an Oversight and Compliance Officer position within the Office of the Assistant Secretary for Cybersecurity and Communications, whose primary function is the monitoring and oversight of the EINSTEIN program. Additionally, DHS's Chief Privacy Officer is part of the development team and is reviewing all components of the EINSTEIN system to determine which elements require a privacy impact assessment (PIA). The Privacy Office will continue to perform thorough privacy analysis and publish as much of the privacy analysis as possible, consistent with security classification.[3] More broadly, the DHS Privacy Office provides privacy training and oversight to US-CERT personnel and the operators of the EINSTEIN system. Furthermore, the DHS Office for Civil Rights and Civil Liberties is participating in the design, planning, and execution of the EINSTEIN program, providing proactive advice on how enhanced cybersecurity efforts may be conducted in a manner consistent with civil rights and civil liberties.

With respect to identity management, the President's Cyberspace Policy Review included the building of "*a cybersecurity-based identity management vision and strategy that addresses*

[3] The PIAs for EINSTEIN 1 and EINSTEIN 2 are publicly available on http://www.dhs.gov/.

privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation" as a near-term priority. The objective is a system that is voluntary, secure, affordable, easy-to-use, and privacy-enhancing. That system should also accommodate a variety of technologies and governance mechanisms, working in an interoperable, decentralized manner. Building that vision and strategy, and including privacy into the design from the beginning, will encourage broad deployment of mechanisms that will reduce identity theft and the theft of other personally identifiable information, and empower the American people to make effective decisions to protect their safety, security and privacy.

Conclusion

In closing, I would like to emphasize that developing and implementing the technical solutions necessary to secure the federal executive branch civilian networks and systems is complicated and requires sophisticated technology. At the same time, these solutions must ensure the continued protection of civil rights, civil liberties, and privacy protections. The President and DHS are committed to transparency and the responsible disclosure of information. We look forward to continuing to work with this Subcommittee and others to ensure that the American people have the information needed to understand the criticality of the systems we protect and the measures in place to mitigate cybersecurity risks.

I appreciate the opportunity to discuss the Department's efforts in advancing our cybersecurity posture and increasing the security of federal networks. I will be happy to answer any questions from the Subcommittee.