Statement for the Record
Of

Secretary Janet Napolitano
U.S. Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

February 16, 2012

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is a pleasure to appear before you today to discuss the critical issue of cybersecurity. I appreciate the opportunity to explain the Department of Homeland Security's (DHS) cybersecurity mission and how new legislation will strengthen our ability to protect the Nation. Specifically, I want to express the Department's strong support for the Cybersecurity Act of 2012. The Department of Homeland Security appreciates the leadership of Chairman Lieberman and Ranking Member Collins, as well as Senators Rockefeller and Feinstein, who have worked in a bipartisan manner over many months and years, to address the core national security requirements and economic interests also laid out in the Administration's legislative proposal. The Cybersecurity Act of 2012 would provide the comprehensive tools we need to effectively address the full range of cyber threats facing our nation, while preserving privacy and civil liberties and respecting freedom, openness, and innovation. As the President noted in the State of the Union address, addressing the dangers of cyber threats is critically important for our nation, and quickly enacting this legislation would be an incredibly important step.

The United States confronts a dangerous combination of known and unknown vulnerabilities in the cyber domain, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse. No country, industry, community or individual is immune to cyber risks. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services.

In addition to risks and vulnerabilities, cyber incidents have increased dramatically over the last decade. There have been instances of theft and compromise of sensitive information from both government and private sector networks, undermining confidence in our systems, information sharing processes, and the integrity of the data contained within these systems. Last year, the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

Recognizing the serious nature of this challenge, President Obama made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, which established a strategic framework for advancing the Nation's cybersecurity policies, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of our entire society—from government and law enforcement to the private sector and most importantly, members of the public. The key question, then, is how do we address this problem? This is not an easy question, because cybersecurity requires a layered approach. The success of our efforts to reduce cybersecurity risks depends on effective communication and partnerships among departments and agencies from all levels of government, the private sector, international entities, and the American public.

RESPONSIBILITIES AND ACCOMPLISHMENTS

DHS works with federal agencies to secure unclassified federal civilian government networks and works with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities. To protect Federal civilian agency networks, we are deploying technology to detect and block intrusions in those agencies with support from the Department of Defense. We also work to provide agencies with assistance in the implementation of guidance and standards issued by the National Institute of Standards and Technology (NIST). In addition, DHS is responsible for coordinating the national response to significant cyber incidents, consistent with the National Response Framework, and for creating and maintaining a common operational picture for cyberspace across the government.

With respect to critical infrastructure, DHS and the sector specific agencies work with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. We do this by sharing actionable cyber threat information with our private sector partners, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident. Last year, the DHS Industrial Control Systems Computer Emergency Response Team (ICS-CERT) conducted 78 assessments of control system entities which helped companies identify security gaps and prioritize mitigations. We also empower owners and operators to help themselves by providing a cyber self-evaluation tool, which was utilized by over 1,000 companies last year, as well as in-person and on-line training sessions.

To combat cyber crime, DHS leverages the skills and resources of the U.S. Secret Service, U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection and works in cooperation with Department of Justice, especially the Federal Bureau of Investigation, to investigate and prosecute cyber criminals. In FY 2011 alone, DHS prevented $1.5 billion in potential losses through cyber crime investigations and announced charges against 72 individuals for their alleged participation in an international criminal network dedicated to the sexual abuse of children and the creation and dissemination of graphic images and videos of child sexual abuse throughout the world.

DHS also serves as a focal point for cybersecurity outreach and awareness efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the personal or financial information of individuals is better protected. As we perform this work, we are mindful that one of our missions is to ensure that privacy, confidentiality, and civil liberties are not diminished by our efforts. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset. DHS has performed Privacy Impact Assessments of our key cybersecurity programs such as EINSTEIN, which provides intrusion detection capabilities to the civilian federal agencies. DHS also receives regular counsel on cybersecurity activities from the Data Privacy and Integrity Advisory Committee (DPIAC), a body of outside experts who advise the Department on ways to address privacy and civil liberties concerns.

CURRENT AUTHORITIES

Congress has granted DHS certain authorities in the area of cyber security. For example, the Homeland Security Act of 2002 specifically directed DHS to enhance the security of non-federal networks by providing analysis and warnings, crisis management support, and technical assistance to State and local governments and the private sector. As part of its critical infrastructure protection mission, DHS also works with the sector specific agencies to carry out vulnerability and risk assessments, identify priorities for protective support measures, and develop a comprehensive national plan for securing the Nation's cyber and communications infrastructure.

Building upon this statutory footing, successive Administrations have assigned the Department key responsibilities in carrying out national cybersecurity efforts. US-CERT has long been designated to carry out the functions of the Federal information security incident center required under the Federal Information Security Management Act (FISMA) to help agencies prevent and respond to cyber incidents on government networks. In July 2010, he Office of Management and Budget assigned DHS primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to Federal information systems.

Several Executive Orders and Presidential Directives have assigned the Department increasing responsibilities related to cybersecurity:

- Executive Order 12472 designates DHS as the Executive Agent for the National Communications System (NCS), which assists the Executive Branch in coordinating the planning and provision of national security and emergency preparedness communications under all circumstances. The NCS is the focal point for joint industry-government national

security and emergency preparedness communications planning, response and restoration during all conditions of crisis or emergency.

- Under Homeland Security Presidential Directive (HSPD) 7, DHS serves as a focal point for the security of cyberspace to facilitate interaction and collaboration between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. DHS also works with the sector specific agencies, as each critical infrastructure sector possesses its own unique characteristics, operating models and risk environment.
- National Security Presidential Directive 54/HSPD 23 directs DHS to manage and oversee consolidated intrusion detection, incident analysis, and cyber response capabilities to better protect Federal networks. DHS also integrates threat and vulnerability information; provides a consultative structure to coordinate the cybersecurity activities of participating Federal cyber centers and ensures that federal agencies have access to information and intelligence needed to execute their respective cybersecurity missions.
- In accordance with HSPDs 23 and 7, DHS disseminates cyber threat, vulnerability, mitigation, and warning information to improve the security and protection of critical infrastructure networks owned or operated by Federal agencies, State, local, and tribal governments; private industry; academia; and international partners.

As its cybersecurity mission continues to evolve, DHS has increased its funding of key programs to keep pace with emerging threats through innovative technologies and services. From FY 2011 to FY 2012, the Department's cyber budget increased by over $80 million or 22 %. The President's FY 2013 Budget request builds on these efforts by making significant investments to expedite the deployment of intrusion detection and prevention technologies on government computer systems, increase federal network security of large and small agencies, and continue to develop a robust cybersecurity workforce to protect against and respond to national cybersecurity threats and hazards. The $769 million FY 2013 budget request for cybersecurity represents a 74% increase over FY 2012.

PARTNERSHIP WITH THE DEPARTMENT OF DEFENSE

The Department of Defense is a key partner in our cybersecurity mission. In 2010, I signed a Memorandum of Understanding with then-Secretary of Defense Robert Gates to formalize the interaction between DHS and the Department of Defense to protect against threats to our critical civilian and military computer systems and networks. Congress mirrored this division of responsibilities in the Fiscal Year 2012 National Defense Authorization Act. We are currently working with the Defense Industrial Base and the Banking and Finance Sector to exchange actionable information about malicious activity. One important goal of the current legislative proposals is to allow DHS to expand and enhance these efforts with critical infrastructure.

WHY NEW LEGISLATION IS NEEDED NOW

While the Administration has taken significant steps to protect against evolving cyber threats, we must acknowledge that the current threat outpaces our current authorities. DHS must execute its portion of the cybersecurity mission under an amalgam of existing statutory and executive authorities that fail to keep up with the responsibilities with which we are charged. Our cybersecurity efforts have made clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated.

Members of both parties in Congress have come to the same conclusion; approximately 30 cyber-related bills have been introduced in the last two Congresses. In addition, Majority Leader Reid and six Senate committee chairs wrote to the President and asked for his input on cybersecurity legislation. The Administration welcomed the opportunity to assist these congressional efforts, and in May 2011 we provided a pragmatic and focused cybersecurity legislative proposal for Congress to consider. We believe these proposals provide important steps in improving the cybersecurity posture of the United States.

Since then, we have had many interactions with this Committee and Congress to provide our perspective. Indeed, in the last two years, Department representatives have testified in 16 committee hearings and provided 161 staff briefings. Given this predicate, we are encouraged that legislation has been unanimously reported from this Committee and from the Commerce Committee. We appreciate that you are holding today's hearing as a public forum to discuss these well-developed legislative issues and applaud the Senate leadership's initiative to take your bill to the Senate floor.

I am pleased to see that recently introduced legislation contains great commonality with the Administration's proposal. Enactment of a bill along these common lines will be a major step forward for the Nation's cybersecurity. Indeed, all sides agree that federal and private networks must be better protected, and information about cybersecurity threats should be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. Both the Administration's proposal and the Senate legislation would improve operations in those areas by providing DHS with clear statutory authority commensurate with our cybersecurity responsibilities. For example, the important updates to FISMA in both the Administration's proposal and yours will enhance the Executive branch's efforts to transform federal network security efforts from costly and ineffective paperwork exercises to implementation of actual security measures.

In addition, many would agree with the House Republican Cyber Task Force when it said, "Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity." Both the Administration's

proposal and the Senate legislation recognize the severity and urgency to secure critical infrastructure and take some basic steps in this area.

Accordingly, the Administration proposed risk mitigation guidance to ensure that companies providing the Nation's most essential services are instituting a baseline level of cybersecurity. This proposal would leverage the expertise of the private sector requiring the Nation's most critical infrastructure adopt the cybersecurity practices, technologies, and performance standards that work best on their networks.

There is also broad support for increasing the penalties for cyber crimes and for creating a uniform data breach reporting regime to protect consumers. The Administration's proposal will help protect the American people by enhancing our ability to prosecute cyber criminals and by establishing national standards requiring businesses that have suffered an intrusion to notify affected individuals if the intruder had access to the consumers' personal information.

I believe we have made great progress toward reaching a consensus that will help protect the American people, Federal government networks and systems, and our Nation's critical infrastructure. I hope that the current legislative debate maintains the bipartisan tenor it has benefitted from so far, and builds from the consensus that spans two Administrations and the Committee's efforts of the last several years.

CONCLUSION

In an election year there is a tendency to put off needed legislation. The threats to our cybersecurity are real, they are serious, and they require urgent action. The current legislation before the Senate has bi-partisan support. Numerous current and former homeland and national security officials have expressed their desire to see it passed this year. The time to act is now: to improve cybersecurity coordination, strengthen our cybersecurity posture, and protect all elements of our economy against this serious and growing threat, while protecting privacy, confidentiality, and civil liberties. We look forward to engaging with Congress in the days ahead to reach agreement on a bill that will move the Nation forward.