

**Statement of Melissa E. Hathaway
before the
House of Representatives Committee on Homeland Security,
Sub-Committee on Cybersecurity, Infrastructure Protection and Security
Technologies**

**“Examining the Homeland Security Impact of the Obama Administrations
Cybersecurity Proposal”**

June 24, 2011

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify on the subject of cyber security and its importance to homeland security. I am appearing today solely in my individual capacity, and not on behalf of any clients or other organizations.

My testimony is divided into three parts: (1) a review of the threat, (2) an assessment of the current legislative docket and the unaddressed needs, and (3) a view on the need to clarify the role of DHS.

Targeted attacks are increasing and our defensive posture remains weak. A sense of urgency is rising because the media reports how our insecure computers are being infected every day. Our opponents harness precision guided bits and bytes to deliver spam, cast phishing attacks, facilitate click-fraud and launch a distributed denial of service (DDoS). The frequency of events and affected people and enterprises are alarming. Recent headlines expose that our money, personal privacy, infrastructure and even our children are at risk. These network intrusions include but are not limited to:

- NASDAQ: The operator of the Nasdaq Stock Market said it found "suspicious files" on its U.S. computer servers and determined that hackers could have affected one of its Internet-based client applications.¹ Investigators are considering a range of possible motives, including unlawful financial gain, theft of trade secrets and a national-security threat designed to damage the exchange.² Impact: Our investment plans and money are exposed.
- Epsilon: Epsilon, which sends 40 billion emails annually on behalf of more than 2,500 clients, detected an incident on 30 March 2011. It determined that a subset of Epsilon clients' customer data were exposed by an unauthorized entry into Epsilon's email system. The information that was obtained was limited to email addresses and/or

¹ Jonathan Spicer. UPDATE 2-Hackers breach Nasdaq's computers. Reuters On line. 5 February 2011. [<http://www.reuters.com/article/2011/02/05/nasdaq-hackers-idUSN0514862120110205>]

² Devlin Barrett. "Hackers Penetrate Nasdaq Computers." The Wall Street Journal. 5 February 2011. [<http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html>]

customer names and represented approximately 2% or 50 customers including Walgreens, Disney destinations, Best Buy, and Citigroup.³ The worry is that even months down the road, customers could get an email impersonating their bank or credit-card issuer containing poisonous Web links. Once clicked, those links could install malicious code on their computers or try to trick them into giving up valuable information, such as credit card information or log-in data to their banks or social media accounts.⁴ Impact: Our personal credentials and privacy are at risk.

- RSA SecureID: In March 2011, RSA informed its customers of a breach of its corporate network which could reduce the effectiveness of its SecureID two factor authentication token. On 21 May 2011, a leading U.S. defense contractor, Lockheed Martin, had its networks penetrated. The perpetrator(s) used duplicates of RSA's SecureID tokens to gain access to Lockheed's internal network.⁵ After this breach and several others resulting from the SecureID issue, RSA Security says it will replace tokens, upon customer request.⁶ Impact: Our trusted transactions (authenticated transactions) are at risk.
- Sony's PlayStation Network was taken down on 20 April 2011. A forensics team investigated the scope of the breach and by May 2nd, the breach reportedly had affected an estimated 100 million people and spread to Sony's Online Entertainment division. In an effort to show how vulnerable Sony was to a breach, the hacker group LulzSec exposed names, birth dates, addresses, emails, passwords, etc. of Sony's customers.⁷ As of the end of May, Sony has spent \$171 million closing the vulnerabilities on its network and informing its customers of their exposure.⁸ Impact: Our children are at risk.
- Citigroup. In early June 2011, computer hackers breached Citigroup's network and accessed the names, account numbers and contact data of hundreds of thousands of bankcard holders in North America.⁹ This may be the largest breach of a financial institution to date, arming criminals with victim data. Impact: Our banks and money are at risk.
- Stuxnet. The Stuxnet worm that was used to shut down Iran's nuclear program has been widely analyzed around the world. It targets control system vulnerabilities and

³ Epsilon. Public Statement by Epsilon. 1 April 2011.

⁴ Ki Mae Heussner. Epsilon Email Breach: What You Should Know. ABC News Online. 4 April 2011. [<http://abcnews.go.com/Technology/epsilon-email-breach/story?id=13291589>]

⁵ Jeffrey Carr. "An Open Source Analysis Of The Lockheed Martin Network Breach." Digital Dao Blog. 31 May 2011. [<http://jeffreycarr.blogspot.com/2011/05/open-source-analysis-of-lockheed-martin.html>]

⁶ <http://www.wired.com/threatlevel/2011/06/rsa-replaces-secuid-tokens/>

⁷ Andy Bloxham. "Sony hack: private details of million people posted online." The Telegraph. 3 June 2011. [<http://www.telegraph.co.uk/technology/news/8553979/Sony-hack-private-details-of-million-people-posted-online.html>]

⁸ Robert Westervelt. "Sony breach timeline shows missteps." Security Bytes online. [<http://itknowledgeexchange.techtarget.com/security-bytes/sony-breach-timeline-shows-missteps-says-security-firm/>] 31 May 2011.

⁹ Maria Aspan. "Regulators pressure banks after Citi data breach." Reuters. 9 June 2011. [http://news.yahoo.com/s/nm/20110609/bs_nm/us_citi]

its source code has been traded on the black market. Security officials worry that this worm will be used again to attack other critical infrastructures that rely on computers and have the same security flaws.¹⁰ Impact: Our critical infrastructure is at risk.

The cybersecurity problem is growing faster than the solution. Upon review of these cases, it can be determined that it costs less to break into a system or enterprise than it does to defend it. An infected thumb drive (USB key) that costs less than \$10 can undermine an enterprise's security in minutes and nullify years worth of information technology (IT) investments. Organizations everywhere are being penetrated -- from small businesses to the world's largest institutions. Policy makers, legislators, and businessmen are assessing the gap between their current defensive posture (the floor) and their needed front line defense (ceiling) in the face of a growing sophisticated range of actors. All of these facts are exasperated by the prolonged economic recovery that has placed significant pressures on enterprise IT budgets and focused actions toward meeting the minimum regulatory requirements like compliance at the expense of broader information security initiatives.

The Comprehensive National Cybersecurity Initiative (CNCI) outlined these multi-dimensional threats along four attack vectors: insider access¹¹, proximity access¹²; remote access¹³; and supply chain access¹⁴ and it provided a framework for unifying investments to shore up the government's defense. President Obama's Cyberspace Policy Review re-stated that the nation must become more resilient to all types of cyber-based attacks. And while there has been activity against many of the recommendations in the Cyberspace Policy Review, there is a lot more that needs to be done.

Cybersecurity in the 111th and 112th Congress.

The 111th Congress considered more than 50 pieces of cybersecurity legislation. The wide range of topics addressed in these bills included proposed changes to organizational responsibilities; instituting compliance and accountability mechanisms; implementing data accountability standards and reporting requirements for personal data privacy, data breach handling and identity theft; enhancing cybersecurity education; advancing research and development grants; evaluating critical electric infrastructure protection and conducting vulnerability analysis of other critical

¹⁰ Stewart Meagher. "Stuxnet worm hits the black market." THINQ. 25 November 2010.

[<http://www.thinq.co.uk/2010/11/25/stuxnet-worm-hits-black-market/>]

¹¹ Unauthorized use or access to information, systems, and networks by otherwise trusted agents (employees).

¹² Gaining access to information or systems via deployment of technology in proximity to the target.

¹³ Accessing target information and/or systems through network-based technical means (Internet).

¹⁴ Gaining advantage, control, and/or access to systems and the information they contain through manipulation by cooperative/witting vendors or unilaterally at any point in the supply chain between the manufacturer and end user.

infrastructures; expanding international cooperation on cybercrime; and addressing procurement, acquisition and supply-chain integrity.

Clearly, cybersecurity is a topic of interest and the sheer number of bills highlights the cross-jurisdictional interest of the subject. The 112th Congress has an opportunity to drive a new legislative conversation and address the shortfalls in our current laws. As of June 2011, at least ten pieces of cybersecurity legislation have been introduced in the United States Senate and at least another nine have been introduced in the United States House of Representatives. Appendix A contains a table that outlines some of the cybersecurity bills under consideration in the 112th Congress. Like many of the bills of the 111th Congress, the bills in the 112th address niches of the cybersecurity problems facing the nation; even if taken together, none of them address the situation in a comprehensive manner.

Cybersecurity legislative proposals reflect different approaches and priorities.

The 21st century digital environment requires new laws that at a minimum address: data ownership; data handling; data protection and privacy; evidence gathering; incident handling, monitoring and traceability; rights and obligations related to data breach and data transfers; access to data by law enforcement or intelligence services; and degree of government assistance (e.g., subsidy, information, technology, liability relief) to close the gap between threat, innovation, and competitiveness. The Cyberspace Policy Review identified scores of laws that needed to be updated. In May 2011, the Administration put forward its cybersecurity legislative proposal. It reflects the efforts of an interagency, consensus based system and a diversity of views across six proposals. Like Congress, it shows the jurisdictional focus by specific mission areas.

Two specific areas of the Administration's package have been debated in the last two sessions of Congress: (1) amending the Federal Information Security Management Act (FISMA) from a static compliance based system to one of continuous monitoring; and (2) providing a federal umbrella to unify guidance of the 47 disparate State data breach laws. The four remaining areas of the Administrations package represent new legislative proposals. Briefly, they seek to: (1) update the Computer Fraud and Abuse Act (CFAA) by stiffening penalties for breaches and theft of information; (2) grant new authorities for DHS--enabling them to deploy Intrusion Prevention Systems (IPS) in the .gov domain and allow DHS to turn to Internet Service Providers (ISPs) to conduct that mission on behalf of the government (with liability relief); (3) establish critical infrastructure regulation, set mandatory standards for "covered critical infrastructures, and an audit and compliance regime that mandates private sector entities to attest to cybersecurity risk management plans; and (4) prevents restrictions on data center locations (i.e., states can't specify that a data center be located in a certain state).

As Congress considers these proposals, it will be important to gain industry's perspective and understand the second and third order effects of the proposals. For example, which sectors will be considered "covered" critical infrastructure, and therefore subject to regulation under the new rules? The President's International Strategy for Cyberspace implies that the Energy, Transportation, Financial Services, and Defense Industrial Base (DIB) sectors will be named the "covered" critical infrastructures. The legislative proposal states, "the owners or operators of covered critical infrastructure shall develop cybersecurity plans that identify the measures selected by the covered critical infrastructure to address the cybersecurity risks in a manner that complies with the regulations promulgated, and are guided by an applicable framework designated."¹⁵ This proposal attempts to establish a minimum standard of care and an audit and certification function that would be similar in kind to the Securities and Exchange Commission (SEC) requirement for attestation of material risks. In my view, inserting DHS into a regulator role in this context could dilute its operational and policy responsibilities and likely detract from the nation's security posture. In May 2011, Senator Rockefeller asked the SEC to look into corporate accountability for risk management through the enforcement of material risk reporting.¹⁶ And in June 2011, Chairman Schapiro said that the SEC would look into the matter. If Congress believes corporations should meet such a reporting requirement then it should turn the Executive Branch Independent Agency that is responsible for this type of reporting and not add an additional mission responsibility to DHS. And while regulation may be necessary, Congress should also consider the use of other market levers (e.g., tax relief, research and development subsidy, etc.) to incentivize industry investment in information security.

Additionally, the Administration is proposing new authorities for DHS by establishing a National Cybersecurity Protection Program (Section 244) that authorizes DHS to actively protect federal systems. The package states, "the Secretary is authorized, notwithstanding any other provision of law and consistent with section 248(a), to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on federal systems and to deploy countermeasures with regard to such communications and system traffic."¹⁷ Of course more active measures must be taken to protect federal systems from cybersecurity threats because passive defenses are simply not enough. The question that Congress needs to carefully consider is which entities in the Government (e.g., Federal Bureau of Investigation (FBI), National Security Agency (NSA), or DHS) are the appropriate

¹⁵ The White House. Cybersecurity Legislative Package: Cybersecurity Regulatory Framework For Covered Critical Infrastructure Act. Page 3.

¹⁶ Senator Rockefeller letter to SEC Chairman Mary Schapiro. 11 May 2011.

¹⁷ The White House. Cybersecurity Legislative Package: Department of Homeland Security Cybersecurity Authority. Page 6.

entities to help secure the federal government systems? Are there appropriate checks and balances in place to oversee these new or extended authorities?

This discussion will become even more important as Congress debates the merits of government involvement in the protection of private sector networks. The Washington Post reported last week that NSA “is working with Internet service providers to deploy a new generation of tools to scan e-mail and other digital traffic with the goal of thwarting cyberattacks against defense firms by foreign adversaries.”¹⁸ Certainly other nations are turning to their ISPs as a front line of defense in protecting their government and private sector networks. But, is this a mission that we want NSA to lead, or is it one that we expect DHS to undertake?

As scary and as problematic as these threats are and intrusions may be (and as devastating as they may be), it is important that the defensive posture not overtake our core freedoms. We should also respect the long standing limitations on the role of the military as it relates to public safety and civilian activities. This is why, in my opinion, the Administration’s legislative package proposes the section (245) for voluntary disclosure of cybersecurity information. It addresses shortfalls in the law and aims to extend the Provider Exception (i.e., 18 U.S.C. § 2511(2)(a)(i)) to include protection against network attacks and prevention of delivery of malware to the end user and provides liability relief for the reporting mechanism back to the government (currently not permitted under the law). One could argue that this is what is being mandated via the code of conduct in Australia and via the recent pan-European telecommunications reform that will be transposed into national laws in the coming months. The European mandate obliges the ISPs to take more responsibility for providing enhanced security services to their customers and report all security incidents to the European Network and Information Security Agency (ENISA).

Clarifying DHS’s role: Policy, Operational, or Regulatory

All of the legislative proposals reflect the dilemma of a co-dependent relationship between the private sector that develops, owns, and operates the internet-based infrastructure for which the government is responsible for delivering essential services (e.g., power, water, telephone, etc.) and ultimately providing economic prosperity and security. Our responses include organizational restructuring, regulation, and attempts to centralize decision making all with the intent to reduce the vulnerabilities and minimize the damages of intrusions. We appear to be asking DHS to take on new cybersecurity roles and missions while it is establishing its basic core competencies. Is this reasonable? Do we want DHS to become a first party regulator? Do we want DHS to assume an operational role that provides actionable information to the private sector

¹⁸ Ellen Nakashima. “NSA allies with Internet carriers to thwart cyber attacks against defense firms” The Washington Post. 7 June 2011.

and provides active defense of federal systems? Or do we want DHS to assume a broader policy role and become the national architect for a more secure and resilient infrastructure? Perhaps it would be better to focus DHS on becoming a center of excellence in one or two areas.

24x7 Information Security Capability (Operational)

Becoming an operational center of excellence that disseminates timely and actionable cybersecurity threat, vulnerability, mitigation and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of federal systems and critical information infrastructure is necessary. To be successful requires DHS to adopt a 24x7 “customer service” business model, where its customers are other federal agencies; State, local, tribal and territorial governments; the private sector; academia and international partners. It would need to learn from successful customer service industries and embed the necessary industry partners (like the member companies of the National Security Telecommunications Advisory Committee) within its operations. It would need to pass knowledge onto its customers that removes the sensitive sources and methods that make it classified and therefore make it more readily available and actionable.

There are many other aspects of a 24x7 information security operation that DHS could take on. Some of these capabilities are outlined in the Administration’s legislative package and some additional capabilities are outlined in other pieces of pending legislation. Yet it is important to admit that establishing an effective 24x7 operation is no small task. It requires real specialization and technical expertise, a commitment to providing a 100% up-time service, and if an incident occurs, an ability to turn to the private entities that will likely be called upon to operate in a degraded state and restore operations (and infrastructures) quickly. While it is possible that the National Cybersecurity and Communications Integration Center (NCCIC) could evolve and assume this role, it would require it to become an independent operational unit carved out of the headquarters entity of DHS--akin to United States Secret Service or the Drug Enforcement Agency.

If we are truly interested in setting up a 24x7 operation immediately, then DHS in cooperation with the Department of Defense (DoD) could call up specialist cybersecurity units within the National Guard or DoD Reserve Forces. DHS could also turn to outside organizations, such as the Carnegie Mellon Computer Emergency Response Team (CERT-CC) to further augment its staff.

National Architect and Advocate for Secure and Resilient Infrastructures (Policy)

Congress and the Administration also turn to DHS raise awareness, fund education initiatives, incubate technology, and broadly set cybersecurity policies for the critical infrastructures. At the forefront, DHS is responsible for increasing public awareness. It is currently sponsoring a competition to develop a public service announcement (PSA) on cybersecurity to augment the October Cybersecurity Awareness Month. It is also conducting a review of the university participation in the National Centers of Academic Excellence in Information Assurance to determine how it can increase the number of

universities participating, obtain full 50 state participation, increase the output of students per program, and align more closely with the National Science Foundation's Scholarship for Service. Linking these programs to hands-on experiential learning like that of the high-school, university, and professional competitions sponsored by the U.S. Cyber Challenge would be a natural next step.

Moreover, DHS's recently released a paper entitled, "Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action" that explores the idea of a healthy, resilient – and fundamentally more secure – cyber ecosystem of the future. It envisions an environment of cyber participants, including cyber devices, that are able to work together in near-real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state.¹⁹ If DHS were to drive the implementation of this vision it will require DHS to modify its relationship with industry, consolidate the number of private-public partnerships, and drive the development of standards in partnership with the National Institute of Standards and Technology (NIST). It will also require DHS to lead the discussion on behalf of the Executive Branch for the following questions: "What are the business drivers that will incentivize the necessary investments? What are the appropriate roles and responsibilities of the public and private sector in delivering the healthy ecosystem? Which elements should be prioritized for early realization? As a healthy cyber ecosystem emerges, governance questions become salient. Will system owners cede decision making to the community? Who sets policy for inter-enterprise information exchange and deployment of countermeasures? What liability regimes apply for collateral consequences of countermeasure deployment (or the failure to deploy known countermeasures)? What legal authorities should local and national governments, as well as international entities, have to compel action by devices owned by or serving private parties in order to secure the larger cyber commons?"²⁰

Like the operational role, this policy based role requires personnel who are steeped with background in policy development and the art of negotiation. It also requires understanding of the technical underpinnings of the next generation hardware and software and knowledge of the standards setting processes. Raising awareness and advocating a new architecture of hardware and software products for industry to build toward is no small task. If Congress and the Administration want DHS to be the national voice for cybersecurity, they cannot necessarily be saddled with all of the operational and regulatory missions that are recommended in the legislative proposals.

First Party Regulatory Role vice Setting Standards

Is it possible for regulation to keep pace with technology development and adoption?
Has the market failed to produce secure and resilient hardware and software products?

¹⁹ Department of Homeland Security. "Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." 23 March 2011.

²⁰ Department of Homeland Security. "Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." 23 March 2011. Page 27.

Many of the critical infrastructures are already regulated (e.g., energy, finance, telecommunications) and NIST works with the Sector Agency and DHS to set the standards by which industry has to meet. But as evidenced by the three volume edition on Guidelines for Smart Grid Cybersecurity,²¹ the standards are not always published in time for market penetration and adoption. So, what is the role of the private sector in policing itself, adapting to new industry standards and upgrades, and coping with accelerating threats? The North America Electric Reliability Corporation (NERC) works across the electric power sector to set the standards and help ensure compliance. However, due to the intermingling of state and federal regulation the industry usually adopts a lower standard leaving some vulnerabilities unaddressed. Existing standards will never be sufficient in light of a sophisticated, perhaps nation state adversary, but they can be strengthened.

What may be more useful would be if DHS, supported by the FBI and intelligence community, were to inform industry of the threats they are facing and how they are being exploited or penetrated. A training program that educates corporate leadership on how to mitigate the risk of being a high value target including providing them with briefings about the threat to their industry using specific case studies may go along way to reducing the number of incidents and loss of confidential information. Furthermore, as some companies are “personally” touched by the penetration of their networks (e.g., Sony and Citigroup), they may be extra motivated to invest in and promote stronger information security standards for their industry and customers alike.

As Congress considers placing DHS into more of a regulatory role, it should consider the impact of the possible dilution of its operational and policy responsibilities. While some say DHS’s input and support of streamlining CIP standards has had a positive affect, is it making enough of a difference? Is it best to educate the first party regulators and help them improve the security posture of the nation? How are the other existing regulatory bodies (SEC, FCC, FERC, or FTC) using their current authorities to address the situation? Would strengthening the regulatory oversight of the SEC, FCC, FERC, or FTC help or hurt the situation?

Conclusion

The 112th Congress has an opportunity to drive a new legislative conversation and address the shortfalls in our current laws. The cybersecurity problem is growing faster than the solution and we cannot afford to be faced with strategic surprise to address the problem. FISMA reform and a national data breach umbrella are needed. Additionally, modern day criminals are using our legal systems’ speed, or lack thereof, to their advantage. We need to stiffen penalties and modernize the laws that are not keeping pace with today’s digital environment. We need to empower the national security community charged with protecting the nation and its critical infrastructure from cyber

²¹ Department of Commerce, National Institute of Standards and Technology. Guidelines for Smart Grid Cyber Security (3 volumes). August 2010.

exploitation or attack. The Computer Fraud and Abuse Act, Electronic Communications and Privacy Act, Stored Communications Act, Telecommunications Act, and Economic Espionage Act are among some of the laws that need to be reviewed and updated. Congress should seek industry's perspective and debate the advantages and challenges associated with fielding a robust active defense capability, imposing standards and regulation on industry, and demanding more of DHS. An overly restrictive approach should be avoided yet, we cannot afford to pass legislation that would prove to be feckless.

* * * * *

I thank you very much for the opportunity to testify, and look forward to your questions.

Exhibit A: Review of Cybersecurity Legislation in the 112th Congress

United States Senate	United States House of Representatives
S. 8, Tough and Smart National Security Act	H.R. 76, Cybersecurity Education Enhancement Act of 2011
S. 21, Cyber Security and American Cyber Competitiveness Act of 2011	H.R. 96, Internet Freedom Act of 2011
S. 28, Public Safety Spectrum and Wireless Innovation Act	H.R. 174, Homeland Security Cyber and Physical Infrastructure Protection Act of 2011
S. 372, Cybersecurity and Internet Safety Standards Act	H.R. 607, Broadband for First Responders Act of 2011
S. 413, The Cybersecurity and Internet Freedom Act of 2011	H.R. 668, Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (SHIELD Act)
S. 709, Secure Chemical Facilities Act	H.R. 1136, Executive Cyberspace Coordination Act of 2011
S. 813, Cyber Security Public Awareness Act of 2011	H.R. 1389, Global Online Freedom Act of 2011
S. 968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act)	H.R. 1540, National Defense Authorization Act for Fiscal Year 2012
S. 1101, Electronic Communications and Privacy Act-- Amendments Act (Digital Privacy Bill)	
S. 1151, Personal Data Privacy and Security Act of 2011	