EXAMINING THE HOMELAND SECURITY IMPACT OF THE OBAMA ADMINISTRATION'S CYBERSECURITY PROPOSAL

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 24, 2011

Serial No. 112–33

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

72–253 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
MO BROOKS, Alabama

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

EXAMINING THE HOMELAND SECURITY IMPACT OF THE OBAMA ADMINISTRATION'S CYBERSECURITY PROPOSAL

Friday, June 24, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, McCaul, Walberg, Long, Marino, Clarke, Richardson, Richmond, and Keating.

Mr. LUNGREN. With the concurrence of the Ranking Member of the full committee, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technology will come to order.

The subcommittee is meeting today to examine the homeland security impact of the administration's cybersecurity proposal.

I would just say at the outset, we have a vote, I guess a single vote, scheduled at about 10:15, so we will have to go over there and then come back. We are going to try and get our opening statements in so that we can proceed directly with our witnesses as soon as we get back from the vote.

I recognize myself for an opening statement.

We are meeting today to examine the impact of the administration's cybersecurity proposal on the Department of Homeland Security. The proposal touches on a number of issues, such as increasing the penalty for hacking, putting in place a comprehensive regime around the issue of large-scale breaches of personally identifiable information, regulating the cybersecurity of the private-sector critical infrastructure owners and operators, and providing needed clarity on the cybersecurity mission of the Department of Homeland Security.

While I may differ on certain elements of their proposal, I am pleased the administration has provided thoughtful inputs to Congress to help us craft an effective National cybersecurity policy. That being said, I believe this proposal is not the end of our effort but the beginning of a much-needed debate on how we, as a Nation, will address these dynamic cybersecurity threats in the future.

With the growing number of computer network cyber intrusions and attacks being reported in the media, the need for strength-

ening cybersecurity is obviously more evident every day. The status quo is not acceptable. The internet and our digital society provide our adversaries multiple attack avenues.

We must continue to innovate and to build a culture of cybersecurity. We must also find a way to incentivize critical infrastructure owners and operators to build security into their business model. Although our Nation faces a difficult fiscal environment, securing our critical infrastructure assets cannot be ignored.

We must be creative and develop ways to improve the return on our security investments. Developing the right liability safe harbors for growing a more robust and mature cyber insurance market won't happen by itself, particularly in this economic downturn. We must tap the talent of the private sector to develop the appropriate ways and means to improve the cybersecurity economic equation. The cost if we don't secure our critical infrastructure and our business networks and data will be far greater.

I thank all of our witnesses for their appearances today. This is the third in our series of hearings on the cyber threat to critical infrastructure.

The administration's proposal outlines their cybersecurity vision, and I, frankly, thank them for it. It will help inform our efforts to develop legislation to better secure our critical infrastructure and Government networks. I am eager to hear how the proposed language would impact those in the private sector, how it would increase the authority of the Department of Homeland Security, and how it positions the Department of Homeland Security to be the focal point of our cybersecurity in the civilian government.

I believe the Department is the appropriate place within the Government to take responsibility for our cybersecurity operations and establish policies and priorities for protecting our civilian departments and agencies. I think having the Government lead by example is critically important.

As Chairman of the House Committee on Administration, I have the cybersecurity responsibility for the House of Representatives. I take that responsibility very seriously and am proud of the job that the CIO and his team have done. Having DHS lead by example is critically important, as I mentioned.

We are going to hear from Dr. Greg Shannon this morning about the future of incident response operations. Carnegie Mellon CERT has long been recognized for its excellence in computer emergency response, and I am hopeful that their experience will help DHS build a world-class computer instant response capability.

I am also honored to have Melissa Hathaway, the former cybersecurity advisor to both President Bush and President Obama, here to discuss the administration's proposal. She was the director of President Bush's Comprehensive National Cybersecurity Initiative. Additionally, as primary author of this administration's 60-Day Cyberspace Policy Review, she is in a unique position to share with us her expertise and perspective on improving the overall cybersecurity enterprise across Government—in particular, how the Government can best interact with private-sector critical infrastructure owners and operators.

I applaud the administration for coming forward with a proposal. They have, I think, some of the answers. I don't think they believe,

nor do I believe, that any one of us has all of the answers. But, together, we can certainly forge ahead to improve from where we are now.

As I mentioned, we have had a vote called. Interesting, we have a little TV screen up here which shows what is going on, but they have managed to put it in mirror fashion so it is reverse of what it says. But I do believe that means we have 11 minutes left. Somebody has invaded our little system here.

But I would like to recognize the Ranking Member from New York, Ms. Clarke, for her opening statement.

Ms. CLARKE. Thank you very much, Mr. Chairman, Ranking Member Thompson, my colleagues, and to the panelists this morning.

We live in a world where it seems that everything relies on computers and the internet. The effective functioning of our critical infrastructure from airports, financial systems, to water systems, factories, the electric grid is highly dependent on computer-based systems called control systems that are used to monitor and control sensitive processes and physical functions.

The danger of both unintentional and intentional cyber attack is real. The potential consequences for an attack on control systems vary widely, from the introduction of raw sewage into potable water systems to the catastrophic failure of critical electrical generators due to the change of a single line of code in the critical system.

We have come to recognize that public-private partnerships are a key component of securing our Nation's computer-reliant critical infrastructure. Private-sector involvement is crucial, as it collectively owns the vast majority of the Nation's cyber infrastructure and is responsible for protecting its networks and systems from the growing threat of a cyber attack. Enhancing the public-private partnerships by developing an improved value proposition and implementing better incentives, among other measures, will be essential to encouraging greater private-sector involvement.

Control systems are not the only computers subject to attack. Every day, thousands of attacks are launched against Federal and private networks by hackers, terrorist groups, nation-states attempting to access classified and unclassified information. The infiltration by foreign nationals of Federal Government networks is one of the most pressing issues confronting our National security. Federal networks have been under attack for years. These attacks have resulted in the loss of massive amounts of critical information, so many of these attacks are classified.

We all know that cybersecurity is a critical National security issue, and this committee has taken the lead. My Ranking Member, Mr. Thompson, reintroduced his cybersecurity bill from last year, H.R. 174, in January of this year and made sure it was referred to this subcommittee. The need to improve America's cyber defense posture is clear, and the Homeland Security Committee has been arguing this point for a long time.

Now the President has come forward with a comprehensive strategy and some legislative proposals about how it will prevent, detect, and respond to attacks on computer systems and infrastructure. There have been many cyber-related bills in the last session

of Congress, and the Members of Congress wrote to the President and asked for his input on cybersecurity legislation. As part of the President's 2-year cyberspace policy review, the White House has put forth a detailed and determined cybersecurity legislative proposal. I look forward to examining that proposal today.

I thank you for calling this hearing, Mr. Chairman, and I yield back the balance of my time.

[The statement of Ranking Member Clarke follows:]

PREPARED STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

JUNE 24, 2011

We live in a world where it seems that everything relies on computers and the internet.

The effective functioning of our critical infrastructure—from airports, financial systems, to water systems, factories, the electric grid—is highly dependent on computer-based systems called "control systems" that are used to monitor and control sensitive processes and physical functions.

The danger of both unintentional and intentional cyber attack is real, and the potential consequences of an attack on control systems vary widely from the introduction of raw sewage into potable water systems to the catastrophic failure of critical electrical generators due to the change of a single line of code in a critical system.

We've come to recognize that public/private partnerships are a key component of securing our Nation's computer-reliant critical infrastructure. Private sector involvement is crucial, as it collectively owns the vast majority of the Nation's cyber infrastructure and is responsible for protecting its networks and systems from the growing threat of a cyber attack.

Enhancing the public/private partnerships by developing an improved value proposition and implementing better incentives, among other measures, will be essential to encouraging greater private sector involvement.

Control systems are not the only computers subject to attack. Every day, thousands of attacks are launched against Federal and private networks by hackers, terrorist groups, and nation-states attempting to access classified and unclassified information, and the infiltration by foreign nationals of Federal Government networks is one of the most pressing issues confronting our National security.

Federal networks have been under attack for years; these attacks have resulted in the loss of massive amounts of critical information, though many of these attacks are classified.

We all know that cybersecurity is a critical National security issue, and this committee has taken the lead. My Ranking Member, Mr. Thompson re-introduced his cybersecurity bill from last year, H.R. 174, in January of this year, and made sure it was referred to this subcommittee. The need to improve America's cyber defense posture is clear, and the Homeland Security Committee has been arguing this point for a long time.

Now, the President has come forward with a comprehensive strategy, and some legislative proposals, about how it will prevent, detect, and respond to attacks on computer systems and infrastructure.

There have been many cyber-related bills in the last session of Congress, and Members of Congress wrote to the President and asked for his input on cybersecurity legislation.

As part of the President's 2-year Cyberspace Policy Review, the White House has put forth a detailed and determined cybersecurity legislative proposal.

I look forward to examining that proposal today, and thank you for calling this hearing Mr. Chairman.

Mr. LUNGREN. I thank the gentlelady.

I now recognize the Ranking Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he may have.

Mr. THOMPSON. Thank you very much, Mr. Chairman, for holding this hearing.

I welcome our witnesses also.

Being, as you have already indicated, that there is a vote on the way, I will submit my opening statement for the record.

[The statement of Ranking Member Thompson follows:]

PREPARED STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JUNE 24, 2011

When President Obama released his Cyberspace Policy Review almost 2 years ago, he declared that the "cyber threat is one of the most serious economic and National security challenges we face . . .".

I agree with him and I am pleased that his administration has taken significant steps to put forth a clear path to update our cybersecurity laws.

I am also pleased we are examining the President's proposal here today.

This committee is the lead on cybersecurity in the House, as it should be, and we have been examining this issue and calling for action since our formation.

I re-introduced my cybersecurity bill, H.R. 174, in January of this year with the continuing hope that it might get a hearing in this committee.

Frankly, the White House proposal we are examining today has used many of the concepts I suggest in my legislation.

We are facing a National and global challenge on cybersecurity, and we must be internationally engaged to make improvements.

Simply put, we must figure out how cyberspace is to be governed, and how it is to be secured. We know that decisions being made by international bodies that govern the internet do not necessarily reflect U.S. National interests.

Major corporations, financial firms, Government agencies, and allies have all been victims of cybersecurity breaches, and these are just the events we know about.

Classified military networks have been penetrated by foreign intelligence agencies, and from the perpetrators' perspective, no one has ever been punished for any of these actions. This is not a record of success.

Since 1998, we have repeatedly tried a combination of information sharing, market-based approaches, public/private partnership, and self-regulation in an effort to strengthen our cyber defenses.

Hopefully, we are learning from the shortcomings of the past and preparing for future challenges.

Mr. Chairman, I look forward to today's examination of the President's proposal, and thank you for calling this hearing.

Mr. LUNGREN. I thank the gentleman for submitting his opening statement.

We will recess until we vote and complete the vote. I believe we just have one vote. So we will return immediately and begin with our witnesses.

With that, this subcommittee hearing is recessed.

[Recess.]

Mr. LUNGREN. The subcommittee will resume.

Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today on this most important topic.

Melissa Hathaway served in President Obama's administration, 2009, where she coordinated the 60-Day Cyberspace Policy Review. Following the report, she stood up the Cybersecurity Office within the National security staff to conduct work based on the blueprint. Previously, she served under President Bush as cyber coordinator executive and director of the Joint Interagency Cyber Task Force in the Office of the Director of National Intelligence. Ms. Hathaway previously worked as principal with Booz Allen & Hamilton; currently is a strategic consultant in the field of cybersecurity.

Mr. Greg Shannon is the chief scientist for the CERT program at Carnegie Mellon University Software Engineering Institute, a Federally-funded research and development center. Mr. Shannon

has previously led applied research and development efforts in cybersecurity and data analysis at a number of private companies as well as the Los Alamos National Laboratory.

Leigh Williams has served as the president of BITS, the technical policy division of The Financial Services Roundtable, since 2007, focusing on improving operational practices and public policy in the financial sector. Previously, he was a senior fellow at Harvard's Kennedy School of Government, researching public- and private-sector collaboration in the governance of privacy and security. In addition, he has worked at Fidelity Investments, where he was the chief risk officer and chief privacy officer.

Then we have Mr. Larry Clinton, president and CEO of the Internet Security Alliance, a multi-sector industry group which was created to integrate advanced technology with the needs of the business community, leading to a secure internet. During his tenure at the Internet Security Alliance, Mr. Clinton created the "Cyber Security Social Contract." He has previously worked as vice president of the USTelecom Association and as legislative director for our former colleague Rick Boucher, who was the subcommittee chair on the Energy and Commerce Committee with jurisdiction over telecommunications and the internet.

We welcome all of you. We would ask you to try and stay within the 5 minutes. Your prepared written text will be made a part of the record.

Before you begin, I would just ask unanimous consent that a letter that we received from the American Chemistry Council in regard to the subject before this committee be made a part of the record.

Without objection, it will be.

[The information follows:]

STATEMENT OF THE AMERICAN CHEMISTRY COUNCIL

JUNE 24, 2011

ACC MEMBERS ARE A CRITICAL ASPECT OF THE NATION'S ECONOMY

The American Chemistry Council (ACC) represents the leading companies in the United States who produce the chemical products essential for everyday life. And, the business of chemistry is a critical aspect of our Nation's economy employing more than 800,000 Americans in good-paying, high-tech positions and produces 20% of the world's chemical products.

More than 96% of all manufactured goods are directly touched by the business of chemistry. The chemical industry provides vital products and materials that help improve our standard of living, advance green energy objectives and protect the health and welfare of all Americans. Our industry produces critical components used in lifesaving medications, medical devices, body armor for our armed forces and law enforcement, energy-efficient light-weight components for vehicles that improve gas mileage, energy-saving building materials, and the durable, light-weight wind turbine blades that help generate green energy that creates jobs while protecting the environment.

CYBERSECURITY IS A TOP PRIORITY FOR ACC AND THE CHEMICAL INDUSTRY

Because of our critical role in the economy and our responsibility to our communities, security continues to be a top priority for ACC members. In 2001, our members voluntarily adopted an aggressive security program that became the Responsible Care® Security Code (RCSC). Responsible Care implementation is mandatory for all members of the ACC and is regularly reviewed by independent, credentialed third-party auditors. The RCSC is a comprehensive security program that addresses physical and cybersecurity risks. The Security Code requires a comprehensive as-

sessment of its cybersecurity vulnerabilities and implementation of appropriate protective measures throughout a company's supply chain, The RCSC has been a model for State-level chemical security regulatory programs in New Jersey, New York, and Maryland and was deemed equivalent to the U.S. Coast Guard's Maritime Transportation Security Act (MTSA).

The Security Code covers the crucial area of cyber and information security and we were gratified that in 2009 the Obama administration made cybersecurity a top priority. Along with physical security, ACC members began actively addressing cybersecurity issues before and after the attacks of September 11, 2001. Cyber experts from member companies also work closely with the DHS National Cyber Security Division (NCSD) in many areas including: National Cyber Storm exercises, information sharing programs, development of the Roadmap to Control Systems Security for the Chemical Sector, A 2009 Program Update can be found on the Obama administration's website—"Making Strides to Improve Cyber Security in the Chemical Sector."

Security in all its dimensions continues to be a top priority for the ACC and the chemical industry, and we're proud of our record of accomplishment and cooperation on cybersecurity with Congress, DHS, and others.

THE CHEMICAL INDUSTRY COMPLIES WITH TOUGH CYBERSECURITY REGULATIONS

On April 9, 2007 the U.S. Department of Homeland Security published the "Chemical Facilities Anti-terrorism Standards" (CFATS) regulatory program. This comprehensive Federal regulatory program requires high-risk chemical facilities to register with DHS, conduct a thorough site security assessment and implement protective measures that comply with 18 risk-based performance standards (RBPS).

In particular, RBPS No. 8 establishes performance standards for cybersecurity that must be implemented by each covered facility. RBPS No. 8 requires facilities to deter cyber sabotage and prevent unauthorized access to critical process control systems including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs) and other sensitive computerized systems. To do this, RBPS No. 8 requires a combination of policies and practices that high-risk chemical facilities must address to effectively secure a facility's cyber systems from attack or manipulation including:

(1) security policy,
(2) access control,
(3) personnel security,
(4) awareness and training,
(5) monitoring and incident response,
(6) disaster recovery and business continuity,
(7) system development and acquisition,
(8) configuration management, and
(9) audits.

In addition, CFATS specifies critical cyber systems that may require certain enhanced security activities including those that monitor and/or control physical processes that contain a chemical of interest (COI); those that are connected to other systems that manage physical processes that contain a COI; or those that contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI.

ACC RECOMMENDATIONS FOR EFFECTIVE CYBERSECURITY POLICIES

ACC and its members support comprehensive cybersecurity legislation that promotes effective collaboration between the chemical industry and the Department of Homeland Security and ensures that robust cybersecurity practices are implemented across the chemical supply chain, while maintaining the free flow of commerce.

To do this ACC recommends the following:

- Create cybersecurity standards that are prioritized based on risk and focused at protecting critical systems that if compromised would truly pose a significant threat to National security, public safety or the National economy. Cybersecurity legislation should establish performance standards to allow for flexibility in their application so that chemical industry entities can use appropriate measures that fit their unique circumstances while ensuring the security of their critical systems. The standards should take advantage of the incredible wealth of knowledge embodied in the international cybersecurity standards community.
- Establish a public/private partnership to effectively share information that is timely, specific, and actionable and is properly protected from public disclosure. Such a partnership will vastly improve the flow of information and ideas to help

quickly identify threats and vulnerabilities. Such an approach will also generate flexible solutions that protect critical cyber systems that operate complex process controls, contain valuable intellectual property and trade secrets and personal information on employees, customers, and suppliers. To help promote the flow of information, information voluntarily provided by the private sector should be adequately protected from public disclosure including Freedom of Information Act requests.

- Provide limited liability protection for the private sector as a result of a cyber-attack, so long as recognized technologies have been applied to address potential threats. In order to promote the more rapid penetration of state-of-the-art emerging technologies to protect against cyber threats, the Government should hold technology users harmless from damages resulting from cyber-attacks on their IT and control systems, so long as recognized technologies have been applied to address potential threats. For example, the liability protections provided by the Safety Act are appropriate to consider. This will in turn provide the private sector better access to more advanced and affordable end products that are safe and secure as possible.
- Strengthen U.S. laws against cybercrimes and aggressively prosecute cyber criminals and promote international cooperation, U.S. laws should be updated and strengthened to protect critical infrastructure from cyber-attacks and hold those accountable for perpetrating said acts that are intended to cause harm to critical infrastructure operating systems, steal intellectual property and trade secrets, or obtain personal information for financial gain.
- Consider the borderless nature of the international cyber community and the challenges that it presents. The U.S. Federal Government should develop strong National and international partnerships to work together in identifying international threats, investigate cyber-crimes, and vigorously prosecute cyber criminals. The American chemical industry is one of the most creative and effective manufacturing enterprises in the world. However, with the advent of the Advanced Persistent Threat (APT), international cyber criminals are attempting to steal our intellectual property with little risk of getting caught. Successful APTs could compromise our industry's ability to compete in the global market place. Without a focused strategy to address this issue, the private sector will continue to fight an uphill battle. ACC encourages the Federal Government to include this issue as a central component of its strategy and strengthen our fight against international cyber theft of intellectual property.

CONCLUSION

We agree that our shared priority is to enhance cybersecurity across the chemical supply chain Nation-wide. ACC looks forward to a productive debate on cybersecurity legislation that protects our critical information infrastructure while promoting effective and efficient commerce that will continue to strengthen our economy.

The members of ACC and the chemical industry are committed to safeguarding America's chemical facilities and the cyber systems that enable their efficient and effective operations. It is in this spirit, that we offer our assistance to work with the DHS and Members of Congress in support of this shared goal.

Mr. LUNGREN. Ms. Hathaway.

STATEMENT OF MELISSA E. HATHAWAY, PRESIDENT, HATHAWAY GLOBAL STRATEGIES, LLC

Ms. HATHAWAY. Thank you, Chairman Lungren, Ranking Member Clarke, Members of the committee, for the opportunity to testify on cybersecurity and its importance to homeland security.

I am appearing today solely in my individual capacity, and I am not representing any clients or other organizations. Please accept my testimony for the record.

My testimony is divided into three sections: It is a review of the threat; it is an assessment of the current legislative docket and unaddressed needs; and a view of the need to clarify the role for the Department of Homeland Security.

Target attacks are increasing, and our defensive posture remains weak. Our opponents harness precision-guided bits and bytes to deliver spam, cast phishing attacks, facilitate click fraud, and launch

a distributed denial-of-service attack. The frequency of events and affected people and enterprises are alarming. Recent headlines will show that our money, our personal privacy, our infrastructure, and our children are at risk.

The NASDAQ breach showed us that our investment plans and money are exposed. The Epsilon breach showed us that our personal credentials and privacy is at risk. The RSA SecureID breach showed us that our trusted transactions and authenticated transactions are at risk. The Sony PlayStation network showed that our children are at risk. Then, finally, the Stuxnet worm showed that our critical infrastructures are at risk.

The cybersecurity problem is growing faster than the solution. The Comprehensive National Cybersecurity Initiative, as well as the Cyberspace Policy Review, highlighted the need to address the threat.

Clearly, cybersecurity is a topic of interest, based on the sheer number of bills that were highlighted in the 111th Congress—over 55 bills—and now in the 112th Congress, showing that a legislative conversation needs to address the shortfalls in our current laws. As of June 2011, at least 10 pieces of cybersecurity legislation have been introduced in the U.S. Senate, and at least another 9 have been introduced in the U.S. House of Representatives. I have highlighted those in my testimony.

The 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, and access to data based on law enforcement and intelligence services.

The administration outlines six proposals that anchor the priorities for debate here in Congress. As Congress considers these proposals, it will be important to gain industry's perspective and understand the second- and third-order effects of these proposals.

For example, which sectors will be covered critical infrastructure and, therefore, be subject to regulation under the new rules? The President's international strategy for cyberspace implies that energy, finance, transportation, and the defense industrial base sectors will be named covered critical infrastructures.

The 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 requirement for attestation of material risk. In my view, inserting DHS into a regulatory role in this context could dilute its operational and policy responsibilities and likely distract from the Nation's security posture.

Additionally, the administration is proposing new authorities for DHS by establishing a National Cybersecurity Protection Program, which authorizes the DHS to explore countermeasures for the overall infrastructure. The discussion will become even more important as Congress debates the merits of Government involvement in the protection of private-sector networks.

As scary and as problematic as these threats are and the 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 longstanding limitations on the role of the military as it relates to public safety and our civilian activities.

I think the most important thing that this committee can address is whether and how we clarify DHS's overall role. Are we going to ask them to be a policy-maker, are we going to be asked them to be a regulator, or are we going to ask them to be an operator?

All of the legislative proposals reflect the dilemma of a co-dependent relationship between the private sector as it develops, owns, and operates the internet-based infrastructure for which the Government is responsible for delivering essential services of power, water, telephone, et cetera, and ultimately providing economic prosperity and security.

Our response includes restructuring regulation and attempts to centralize decision-making, all with the intent to reduce vulnerabilities and minimize the damages of intrusion. My testimony reflects different ideas on each of the roles: Operational, regulatory, and policy.

In conclusion, the 112th Congress has an opportunity to drive a new legislative conversation and address the shortfalls in current laws. The cybersecurity problem is growing faster than the solution, and we cannot afford to be faced with strategic surprise to address this problem. FISMA reform and a National data breach umbrella are needed.

Additionally, modern-day criminals are using our legal system's speed and lack thereof to their advantage. We need to stiffen the 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 exploitation or attack.

The Computer Fraud and Abuse Act, the Electronic Communications and Privacy Act, the Stored Communications Act, the Telecommunications Act, and the 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 and active defense capability, imposing standards and regulation on industry, and demanding more of DHS. An overly restrictive approach should be avoided. We cannot afford to pass legislation that would prove to be feckless.

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

[The statement of Ms. Hathaway follows:]

PREPARED STATEMENT OF MELISSA E. HATHAWAY

JUNE 24, 2011

Mr. Chairman and Members of the committee: Thank you for the opportunity to testify on the subject of cybersecurity 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 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 2, 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 its source code has been traded on the black market. Secu-

---

[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-idUSN05148621-20110205*.

[2] Devlin Barrett. "Hackers Penetrate Nasdaq Computers." The Wall Street Journal. 5 February 2011. *http://online.wsj.com/article/SB10001424052748704709304576124502351-634690.html*.

[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-securid-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 on-line. *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*.

rity 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 multidimensional threats along four attack vectors: Insider access,[11] proximity access;[12] remote access;[13] and supply chain access [14] 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. 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 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.

---

[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.

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 administration's 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 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 cyber-attacks against defense firms by foreign adversaries."[18] Certainly other nations are turning to their ISPs as a front line of defense in protecting

---

[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.

[18] Ellen Nakashima. "NSA allies with internet carriers to thwart cyber attacks against defense firms" The Washington Post. 7 June 2011.

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 decisionmaking 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 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.

24×7 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 24×7 "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 24×7 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 24×7 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 24×7 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 decisionmaking 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?

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 Cor-

[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.

[21] Department of Commerce, National Institute of Standards and Technology. *Guidelines for Smart Grid Cybersecurity* (3 volumes). August 2010.

poration (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 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.

REVIEW OF CYBERSECURITY LEGISLATION IN THE 112TH CONGRESS—
Continued

United States Senate	United States House of Representatives
S. 968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act). S. 1101, Electronic Communications and Privacy Act—Amendments Act (Digital Privacy Bill). S. 1151, Personal Data Privacy and Security Act of 2011.	H.R. 1540, National Defense Authorization Act for Fiscal Year 2012.

Mr. LUNGREN. Thank you very much for your testimony.
Now Dr. Shannon.

STATEMENT OF GREGORY E. SHANNON, CHIEF SCIENTIST FOR COMPUTER EMERGENCY READINESS TEAM (CERT), SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

Mr. SHANNON. Thank you, Chairman Lungren, Ranking Member Clarke, and other Members of the subcommittee, for me to talk about, this morning, the future of cyber incident response. I applaud the current efforts of Congress to mitigate risks to our public and private critical information infrastructures.

CERT, as you mentioned, is a Federally-funded Department of Defense research and development lab. We have over 250 staff that have been working on this challenge of incident response since 1988, when the Morris worm first was experienced. For example, we catalogue over a quarter-million malware artifacts each month. We assist in major, on-going cybersecurity incidents of National importance. We release security coding guidelines and technologies for the C, C++, and Java programming languages.

While much is said about risk mitigation, incident response receives less focused attention as a strategic technical area, yet it is critically important. Vigorous attacks on our network environments will continue for the foreseeable future, failures will occur, and effective responses are required. The Federal Government must look at incident response as strategic, just as it looks at preventative efforts. The U.S. CERT and other capabilities are a part of this effort.

Our country needs legislation that will facilitate capable, scalable, cost-effective cybersecurity incident response for critical Government infrastructure. Things will fail in unexpected ways, and our Nation must have the capacity to respond accordingly.

I believe that the most difficult technical challenge to both effective risk mitigation and incident response is selecting practices that are scientifically sound and operationally proven. We do not want to be guessing. I encourage you to consider in the rulemaking language that valid approaches be considered. The complexity of practices and regimes being proposed will probably have unintended and unexpected consequences. Some approaches aren't fully proven, experimentally or operationally. Again, I encourage you to use language that calls that out in the rulemaking.

I believe that the most difficult policy challenge for effective Government incident response is harmonizing the responsibilities, authorities, capabilities, and communication across the various agencies, as Ms. Hathaway has highlighted. At CERT, part of our value to the Government has been the ability to bridge these gaps and misalignments in the midst of the response to a critical cybersecurity incident. But we recognize that that is not the ideal way, going forward, to be ad hoc.

Three areas that we highlight in the written testimony is: Data sharing, forensics, and training. I would encourage—I applaud the effort of safe harbors in Section 246 for organizations and individuals that are attempting to do the right thing. The notion of "right thing" in incident response is a well-founded principle that individuals, organizations often know what the right thing to do is, and it is important that the policies and such be aligned to support that.

On the forensics side, what we are seeing is an excellent use of potential cloud-based computing, private clouds, to support a broad capability for the law enforcement community to do investigations at scale. As these incidents increase in scope and scale, the ability to respond quickly with appropriate forensics, to maintain the velocity of the investigation, as well as to collect the evidence that could be used in court, is important.

Finally, on training, one of the key challenges is how to train as the technical people work, or, as the Department of Defense says, train as you fight. The environments that we are in are complex. The threats that are experienced are even more complex and less likely to be experienced. Part of the work we do is to encourage the "train as you work" mentality, to be realistic.

We at CERT look forward to the day when our Nation's cybersecurity resiliency is founded on the effective mitigation of cyber risks and pervasive capabilities to respond to cybersecurity incidents. I see this legislation and the related modifications and efforts as an important step in the right direction.

For your benefit, I would like to also submit an article from Nature. It talks about the Stuxnet. This was in the June issue. At the end of it, it highlights some of the technical challenges from a science-of-security point of view. I would like to also submit that into the written record.

Mr. LUNGREN. Without objection, that shall be accepted.*

Mr. SHANNON. Okay. Thank you for your time.

[The statement of Mr. Shannon follows:]

PREPARED STATEMENT OF GREGORY E. SHANNON

JUNE 24, 2011

Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee, thank you for the opportunity to testify, it is my pleasure to be here this morning to discuss cyber incident response.

*The information has been retained in committee files and is available at *http://www.nature.com/news/2011/110608/full/474142a.html*.

ABOUT CERT®

The CERT Program is part of Carnegie Mellon University's Software Engineering Institute, a Federally-funded research and development center, and is located on the Carnegie Mellon campus in Pittsburgh, Pennsylvania.

The CERT program *(http://www.cert.org/)* was charged by DARPA in 1988 to set up the first Computer Emergency Response Team (CERT) as a response to the Morris worm incident. We continue to develop and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, and restore continuity of critical services. CERT works both to mitigate cyber risks and coordinate cyber incident responses at local, National, and global levels. Over the last 23 years CERT has helped to establish over 200 CERT computer security incident response teams (CSIRTs) around the world—including the DHS US–CERT. We continue to have proven success transitioning research and technology to those who can implement it on a National scale.

Dr. Greg Shannon is the Chief Scientist for the CERT Program, where he works to establish and enhance the program's research visibility, initiatives, strategies, and policies.

TESTIMONY

Today's operational cyber environments are complex and dynamic. User needs and environmental factors are constantly changing, which leads to unanticipated usage, reconfiguration, and continuous evolution of practices and technologies. New defects and vulnerabilities in these environments are continually being discovered, and the means to exploit these environments continues to rise. The CERT Coordination Center cataloged ~250,000 instances of malicious artifacts last month alone. From this milieu, public and private institutions respond daily to repeated attacks and also to the more serious previously un-experienced failures (but not necessarily unexpected); both demand rapid, capable, and agile responses.

Incident response, as a discipline, is maturing. Over the last two decades, it has emerged from the shadows of IT and risk management, to achieve recognition as a robust and growing discipline.[1] Signs of this progress include the emergence of process models, meta-models, bodies of knowledge, common data representations, and auditable standards. Further development, and continued funding, will enable faster and more efficient dissemination of information to trusted partners in larger trust networks.

I applaud the current efforts of the Federal Government to mitigate risk to our public and private critical information infrastructures; CERT has worked tirelessly to improve cybersecurity in areas such as secure coding, insider threat, and vulnerability analysis. But, while much is said about risk mitigation, incident response is often not as thoroughly addressed, and is critically important. Networked environments will continue to be vigorously attacked for the foreseeable future. Failure will occur and effective responses are required. Incident response is not a single action but rather a complex function that includes containment, repair, and recovery.[2] The Federal Government must look at incident response as strategic, just as it looks at preventative efforts. Our country needs legislation that will facilitate capable, scalable, and cost-effective cyber-incident response for critical and Government infrastructure. Things will fail in unexpected ways and our Nation must have the capacity to respond accordingly.

I believe that the most difficult technical challenge to effective risk mitigation and incident response is selecting practices that are scientifically sound and operationally proven. The complexity of practices and regimes being proposed in legislation and elsewhere will probably have unintended and unexpected consequences. I encourage the subcommittee to use language in legislation that encourages practices that are both experimentally and operationally validated.

I believe that the most difficult policy challenge for effective Government incident response is harmonizing the responsibilities, authorities, capabilities, and communication across the various agencies involved. I support the current efforts in this.

In my remaining testimony I discuss three areas that we at CERT believe are key to the future of incident response.

---

[1] For example, this fall, CERT and the Institute for Information Infrastructure will hold a workshop on Coordinated Private-Sector Responses to Cyber Security Incidents. This is a follow on to I3P's 2009 workshop on Protecting Critical Infrastructures: The National Capital Region as a Model for Cyber Preparedness.

[2] Some contend that retaliation is part of incident response; I disagree. The response community does not consider it in scope for incident response as practiced today. Other organizations and disciplines are better suited to address this issue.

INFORMATION SHARING

We all realize how critical it is for stakeholders to share information, but good incident response is contingent upon sharing the right information, with the right people, at the right time. High-quality and actionable information comes from superior situational awareness only possible with robust information sharing and sufficient visibility into one's own enterprise. Currently, our technical capabilities allow us to see and respond to variant indicators, but to better detect, share, and respond to incidents analysts need to be able to look past narrowly-focused indicators.

Achieving this enhanced situational awareness will require continued research on network traffic and data. The ability to detect malicious markers that are invariant, such as behavioral-based indicators (e.g. insider threats) will enable a more proactive response. To facilitate innovation, richer data needs to be shared with the research community, not only incident data itself, but also data-sets that will enable an understanding of what "normal" resembles. Currently, the community does not have a clear understanding of what this data set would look like. If situational awareness is to develop beyond simple indicators, regulatory frameworks must allow access to everyday data, so that investigators can begin to recognize what data-set are important. This data sharing should start with limited access to high-fidelity data sets for researchers so that data with scientifically proven value is considered for sharing operationally. Otherwise, policymakers and experts are left to speculate what is the right data to share. To further improve the future efficiency and effectiveness of incident response, the community also needs to develop and use automated tools and techniques to analyze and correlate the vast amount of log files, artifacts, and other event information.

Moreover, compliance-driven information sharing will only lead to the bare minimum disclosure of sensitive information related to problems, concerns, and vulnerabilities. Building trusted relationships with stakeholders becomes essential to avoiding such limited information exchange and is a fundamental ingredient to a successful response. We also have to trust the people in the field and those who first respond to incidents. I applaud the effort in this legislation to support actions to do the "Right Thing™"; this is an important principle in the response community and is the basis of successful responses in many highly stressful incidents. Safe harbor measures such as Sec. 246 in the administration's Cybersecurity Legislative Proposal work towards continued encouragement to share data; however in response scenarios it is worthwhile to consider including the actions of cyber "first responders" into good faith legislation as well.

FORENSICS

While gains have been made in the field of incident response the nature of the ever-evolving cyber threat poses a huge challenge and demand for incident response expertise that has far outstripped the supply.

Computers are no longer just the targets of crime; our adversaries now use them to facilitate every aspect of their illicit activities and achieve effects at scale. Once an incident occurs Federal agencies are facing several hurdles to recover the needed data in order to locate the source of the incident and contain the problem. First, computer forensic labs are constrained by a lack of resources, creating an enormous backlog rendering them unable to handle the megafold increases in the volumes of data that need to be examined for evidence. While some agencies may have the qualified examiners, and many do not, they lack the funds to properly equip them for the mission. For example, current examination methods rely heavily on processor power, but due to dramatically increased computer memory, examination stations often cannot keep up. Finally, the current state of the practice does not allow examiners to easily access varied levels of expertise in a timely or cost-effective way; frequently people are sent Temporary Duty or images are shipped to higher level units, resulting in time delays and increased costs.

To successfully respond to cyber incidents these obstacles must be overcome in a way that allows for high-quality collaborative examinations. For instance, what would happen if an adversary perpetrated an actual, severe cyber event with National consequences? Currently there is no one facility or lab that could support the volume of data these kinds of events would generate. Under current conditions, data would have to be distributed, adding to the time and complexity of conducting examinations. Agencies will need to augment scarce resources by having multiple users viewing the same data either remotely or locally, while maximizing the application of specialized computing resources, and allowing for massive, coordinated efforts. Analysts and investigators will need flexible, secure access to high-performance systems, to increase productivity and facilitate effective distributed collaboration in a scalable and cost-effective way.

TRAINING

In order to rapidly handle cyber incidents the Federal Government needs a workforce educated and equipped to respond. However, the rapid changes and dynamic nature of cybersecurity make keeping the workforce up to date a very challenging problem. Responding to critical cyber events requires technical knowledge and skills, decision-making abilities, and effective coordination—all while moving rapidly. Moreover, a lack of preparation inhibits secondary incident-handling activities, such as: Evidence gathering, identifying the attacker, and reporting the incident to other affected organizations. The Federal Government must have an agile and prepared workforce to deal with cyber incidents, and should to be able to train them in a cost-effective and scalable manner.

The most common workforce development training solution is the traditional classroom training model. While this training model is easy to implement and is widely used, there are a number of reasons why it is not adequate for providing effective, large-scale training to a technical workforce, including time, cost, and scalability. Furthermore, traditional classroom training is not optimal for rapidly-changing fields such as cybersecurity.

The best way to prepare the workforce is to have them practice under realistic conditions with interactive simulations, and the ability to interface with participants across multiple locations who can work together to analyze and respond to the latest threats and attacks. Individuals need to be trained on a platform that safely mimics how the internet would respond to stress and exposes them to real-world scenarios, events, and activities that are similar to those they will encounter in their jobs.

In addition, there are two incident response domains where we see an immediate need for further training. The first is reverse engineering, to grow capacity in analyzing malware recovered from an incident. The second domain is embedded systems, which pose many unique challenges for incident response and which some experts believe will be a major cybersecurity problem area in the near future.

The workforce needs to not only be trained, but also educated. For example, in the case of forensics, much of the training the workforce receives is how to use tools, but when those tools are not effective no one is educated on how to manage the situation or apply critical thinking to determine alternative approaches. What's more, to train the workforce to manage cyber incidents the Federal Government needs to expand the scope of computer or cybersecurity training to include first responder training and best practice guidance. Without proper education a first responder may unintentionally cause irrevocable damage by doing something as simple as turning off a computer. This will not only cause lost data, but can also result in severely slowing an investigation and compromise the potential prosecution of the perpetrator.

In conclusion, I thank the subcommittee again for inviting me and considering my testimony. Our Nation will continue to see significant serious cyber incidents for the foreseeable future. CERT's mission is to help ensure that these incidents are not catastrophic and that we recover as quickly as possible. We at CERT look forward to the day when our Nation's cyber resiliency is founded on the effective mitigation of cybersecurity risks and pervasive capabilities to respond to cybersecurity incidents. I see this legislation and the related modifications and efforts as an important step in the right direction.

Mr. LUNGREN. Mr. Williams.

STATEMENT OF LEIGH WILLIAMS, PRESIDENT, BITS, THE FINANCIAL SERVICES ROUNDTABLE

Mr. WILLIAMS. Thank you, Chairman Lungren, Ranking Member Clarke, and Members of the committee.

My name is Leigh Williams, and I am president of BITS, the technology policy division of The Financial Services Roundtable, where we address security fraud and other technology issues on behalf of our 100 member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

In my remarks today, I will briefly describe cybersecurity in financial services, explain why The Roundtable supports the Obama administration's cybersecurity legislation, and comment on some of the strong provisions of H.R. 174.

In my view, most cybersecurity protection arises from individual institutions investing literally tens of billions of dollars and tens of millions of hours in voluntary measures for business reasons. Up at the industry level, BITS and several other coalitions promote best practices for protecting customer information. For example, BITS is currently addressing security in mobile, cloud computing, social networking, protection from malicious software, and security training and awareness.

Beyond these voluntary efforts, our members are also subject to a range of oversight mechanisms to ensure consistency throughout the industry. Just to take security and privacy provisions of Gramm-Leach-Bliley as an example, Congress enacted GLB; the banking regulators detailed it in Reg P; Reg P was translated into examination guidance; banks used that guidance to manage their risk and the risk of their service providers; examiners audit the banks against it; Treasury monitors their consistency; and then just to bring this whole process full circle, the Congress oversees Treasury and the agencies.

Beyond this sector-specific work, we collaborate more and more with DHS, with law enforcement, with the intelligence community, and with other industries on a variety of projects, including one that we have launched recently with DHS, the Cyber Operational Resiliency Review, where institutions can invite DHS to review their control practices and their network traffic.

As the committee considers action on cybersecurity, I would urge Members to appreciate these current safeguards and these existing collaborations so that we might leverage all of them for maximum benefit.

Even given this headstart, we believe that comprehensive cybersecurity legislation is warranted. It can improve security throughout the cyber ecosystem, including in telecom networks, in software and hardware supply chains, in Federal systems, and in our sector.

Specifically, The Roundtable supports the administration's legislative proposal. We support many of the provisions on their individual merits, and we see the overall proposal as an important first step in building a more integrated approach.

We do believe that harmonizing the comprehensive approach and the sector-specific mechanisms will be a challenge. There are at least a couple of ways of bridging this ecosystem sector divide. First, Congress could establish uniform standard but with exceptions where substantially similar requirements already are in place, as in the banking regulators' breach notification rules. Or Congress could reserve more autonomy for the sectors. For example, it could be the sector-specific agencies, and not DHS, that designate the critical sector entities or systems or assets.

In other specific provisions of the proposal, we support strengthening penalties for computer crime, including the theft of intellectual property. We support a uniform national standard for breach notification with strong preemption. And we support the Federal systems provisions, both to safeguard the data that we report and to the systems and because we believe, as the Chairman has suggested, that Government should use its procurement power to model good behavior.

On H.R. 174, the Homeland Security Cyber and Physical Infrastructure Protection Act, we see two more promising options for harmonizing DHS and sector-level work. DHS can delegate authority to the sector, and DHS is instructed to use the primary regulators as conduits to the covered companies. With these options, delegation and conduit, and the options in the administration proposal already in place, and sector plus aggregation, we should be able to take full advantage of both the sector and DHS. Finally, we appreciate H.R. 174's focus on risk-based performance-based regulation, on R&D, and on information-sharing among the critical companies and key agencies.

In conclusion, may I just say that at The Financial Services Roundtable we will continue to strengthen security around our customers' information, we will help answer the question of ecosystem sector balance, and we will support and we will work to implement the administration's cybersecurity proposal.

Thank you very much for your time.

[The statement of Mr. Williams follows:]

PREPARED STATEMENT OF LEIGH WILLIAMS

JUNE 24, 2011

Thank you Chairman Lungren, Ranking Member Clarke, and Members of the committee for the opportunity to testify before you today.

My name is Leigh Williams and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology, and public policy, on behalf of its 100 member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

From this perspective, I will briefly describe cybersecurity and data protection in financial services, including private sector efforts, sector-specific oversight and intersector interdependencies. I will explain why The Financial Services Roundtable supports the cybersecurity proposal delivered by the Obama administration to the Congress on May 12. Finally, I will comment on the key provisions of H.R. 174, which I understand is under active consideration by the committee.

FINANCIAL INSTITUTIONS' VOLUNTARY CYBERSECURITY EFFORTS

Within the financial services sector, the greatest amount of cybersecurity protection arises from voluntary measures taken by individual institutions for business reasons. To protect their retail customers, commercial clients and their own franchises, industry professionals—from Chief Information Security Officers to CIOs to CEOs—are increasingly focused on safeguards, investing tens of billions of dollars in data protection. They recognize the criticality of confidentiality, reliability, and confidence to their success in the marketplace. This market-based discipline is enforced through an increasingly informed consumer base, and by a very active commercial clientele that often specifies security standards and negotiates for audit and notification rights.

At the industry level, BITS and several other coalitions facilitate a continuous process of sharing expertise, identifying and promoting best practices, and making these best practices better, to keep pace in a dynamic environment. For example, as BITS and our members implement our 2011 business plan, we are addressing the following items associated with protecting customer data:

- Security standards in mobile financial services.
- Protection from malicious or vulnerable software.
- Security in social media.
- Cloud computing risks and controls.
- Email security and authentication.
- Prevention of retail and commercial account takeovers.
- Security training and awareness.

While much of this institution-level and industry-level effort is voluntary—not driven primarily by regulation—it is not seen by industry executives as discre-

tionary or optional. The market, good business practices and prudence all require it.

OVERSIGHT

To strengthen public confidence and to ensure consistency across a wide variety of institutions, Federal financial regulators codify and enforce an extensive system of requirements. Many of these represent the distillation of previously voluntary best practices into legislation introduced in Congress, enacted into law, detailed in regulation, enforced in the field, with feedback to the Congress in its oversight capacity.

In addition to these Federal authorities, institutions are subject to self-regulatory organizations like the Financial Industry Regulatory Authority (FINRA), State regulators like the banking and insurance commissioners, independent auditors, outside Directors, and others.

These various oversight bodies, for example, apply the Financial Services Modernization Act of 1999 (GLB), the Fair and Accurate Credit Transactions Act (FACTA), Electronic Funds Transfers (Regulation E), Suspicious Activity Reporting (SARs), the International Organization for Standardization criteria (ISO), the Payment Card Industry Data Security Standard (PCI), BITS' own Shared Assessments and many, many more regulations, rules, guidelines, and standards.

INTER-SECTOR COLLABORATION

Commensurate with the escalating cybersecurity challenges and increasing interconnectedness among sectors, more and more of our work entails public/private and financial/non-financial partnerships. Our Financial Services Sector Coordinating Council (FSSCC) of 52 institutions, utilities, and associations actively partners with the 17 agencies of the Finance and Banking Information Infrastructure Committee (FBIIC). [For additional detail on the FSSCC's perspective on cybersecurity, research and development, and international issues, please refer to the April 15, 2011 testimony of FSSCC Chair Jane Carlin before this subcommittee.] Our Financial Services Information Sharing and Analysis Center (FS–ISAC) is in constant communication with the Department of Homeland Security (DHS), law enforcement, the intelligence community and ISACs from the other critical infrastructure sectors, to address individual incidents and to coordinate broader efforts.

Other examples of collaboration with non-financial partners, drawn just from BITS' 2011 agenda, include:

The Cyber Operational Resiliency Review (CORR) pilot, in which institutions may voluntarily request Federal reviews of their systems, in advance of any known compromise—with DHS and the Treasury.

Multiple strategies for enhancing the security of financial internet domains—with the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign, in partnership with the American Bankers Association (ABA) and in consultation with members of the Federal Financial Institutions Examination Council (FFIEC).

A credential verification pilot—with DHS and the Department of Commerce—building on private sector work that began in 2009, was formalized in a FSSCC memorandum of understanding in 2010, and was featured in the April 15, 2011 announcement of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Through the processes and initiatives above and in many other efforts, financial institutions, utilities, associations, service providers and regulators continue to demonstrate a serious, collective commitment to strengthening the security and resiliency of the overall financial infrastructure. As the committee considers action on cybersecurity, I urge Members to be conscious of the protections and supervisory structures already in place and the collaborations currently underway, and to leverage them for maximum benefit.

NEED FOR LEGISLATION

Even given this headstart and substantial momentum, we believe that cybersecurity legislation is warranted. Strong legislation can catalyze systemic progress in ways that are well beyond the capacity of individual companies, coalitions, or even entire industries. For example, comprehensive legislation can:

Raise the quality and consistency of security throughout the full cyber ecosystem, including the telecommunications networks on which financial institutions depend.

Enhance confidence among U.S. citizens and throughout the global community.

Strengthen the security of Federal systems.

Mobilize law enforcement and other Federal resources.

Enable and incent voluntary action through safe harbors and outcome-based metrics, rather than relying primarily on static prescriptions.

Attached are a list of 13 policy approaches that the FSSCC recently endorsed, along with three that it deemed problematic. We urge the committee to consider the FSSCC's input, particularly in light of the FSSCC's leadership of the financial services industry on this issue.

ADMINISTRATION PROPOSAL

On May 12, 2011, on behalf of the administration, the Office of Management and Budget transmitted to Congress a comprehensive legislative proposal to improve cybersecurity. The Financial Services Roundtable supports this proposal and looks forward to working for its passage. We support many of the provisions of this proposal on their individual merits, and we see the overall proposal as an important step toward building a more integrated approach to cybersecurity. Given that our member institutions operate Nationally, are highly interdependent with other industries, and are already closely supervised by multiple regulators, we appreciate that this proposal promotes uniform National standards, throughout the cyber ecosystem, with the active engagement of sector-specific agencies and sector regulators.

Consistent with its comprehensive approach, the proposal strives to address cybersecurity both at the level of the entire ecosystem and also within specific sectors. For example:

The DHS Cybersecurity Authority title naturally stresses DHS' role, but it also mentions "other relevant agencies" and sector coordinating councils.

The Regulatory Framework title focuses largely on DHS leadership and standardized evaluations, but it also mentions ISACs and sector-specific regulatory agencies, and provides for sector-level exemptions.

We believe that harmonizing the comprehensive approach with the need to incorporate sector-specific mechanisms will be one of the most important challenges as the Congress considers this proposal. As this committee considers DHS' role, and its relationship to the sector-specific roles, we urge Members to leverage existing financial services protections and circumstances, and their analogs in other sectors, while preserving the inter-sector quality of the proposal. Below, we offer the committee two potential approaches and illustrations for addressing this DHS/sector nexus:

- *Establish a uniform standard with specified exceptions*.—In the Data Breach Notification title, the Federal Trade Commission (FTC) could enforce the requirements enacted under this bill, but defer to sector-specific regulators where substantially similar sector-specific rules and guidelines already are in place (e.g. the FFIEC could continue to enforce its 2005 interagency breach response guidance, and the Department of Health and Human Services could continue to enforce HITECH).
- *Preserve sector autonomy with centralized information aggregation and coordination*.—In the Regulatory Framework title, rather than requiring DHS to list critical infrastructure entities for every sector, the sector-specific agencies could make that determination, just as the Financial Stability Oversight Council is responsible for designating Systemically Important Financial Institutions.

Given the likely fluidity of the overall solution, we cannot yet make a definitive recommendation for either approach. We do believe that this question of ecosystem/sector balance warrants careful deliberation.

Law Enforcement

We support the proposal's clarification and strengthening of criminal penalties for damage to critical infrastructure computers, for committing computer fraud, and for the unauthorized trafficking in passwords and other means of access. We also urge similar treatment for any theft of proprietary business information. With this extension to intellectual property, the law enforcement provisions will improve protections for both consumers and institutions, particularly when paired with expanded law enforcement budgets and the recruitment of personnel authorized in later titles. For purposes of this title and others, we presume that many, but not all, financial services systems and entities will be designated as critical infrastructure vital to National economic security, and we look forward to further work on the associated criteria.

Data Breach Notification

We support the migration to a uniform National standard for breach notification. Given existing State and financial services breach notification requirements, this migration will require both strong pre-emption and reconciliation to existing regula-

tions and definitions of covered data. [Please see the 2005 FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.] We support the exemptions for data rendered unreadable, in breaches in which there is no reasonable risk of harm, and in situations in which financial fraud preventions are in place.

DHS Authority

We support strengthening cybersecurity authorities within DHS—and the active collaboration of DHS with the National Institute of Standards and Technology (NIST), sector-specific agencies such as the Treasury Department, and sector regulators such as our banking, securities, and insurance supervisors. This title demonstrates both the administration's commitment to an integrated approach and the challenge of achieving it. Federal and commercial systems, financial and non-financial information, DHS planning and sector coordinating council collaboration, are all addressed here and all will need to be very carefully integrated. Within financial services, we are conscious of the many current mechanisms for oversight, information-sharing and collaboration, but we are also conscious of the need for better alignment with our partners in other sectors. We look forward to further work in this area of integration and harmonization, at both the legislative and implementation stages.

We also believe that two areas mentioned in this section—fostering the development of essential technologies, and cooperation with international partners—merit considerable investment. As DHS and NIST pursue their research and development agenda, and as the administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas.

Regulatory Framework

We support all of the purposes of this section, including, especially: The consultation among sector-specific agencies, regulators, and infrastructure experts; and the balancing of efficiency, innovation, security, and privacy. We recognize that giving DHS a window into financial services' cybersecurity risks, plans, and incident-specific information is an important element of building a comprehensive solution. Reconciling all of these elements—Treasury and our regulators' sector-specific roles, DHS' integration role, and the dual objectives of flexibility and security—will be critically important if we are to capitalize on existing oversight, avoid duplication, and avoid the hazards of public disclosures of sensitive information.

Federal Information Security Policies

We are encouraged by the proposal of a comprehensive framework for security within Federal systems. As institutions report more and more sensitive personal and financial data to regulators (and directly and indirectly to DHS), it is critically important that this data be appropriately safeguarded. Protecting this data, modeling best practices, and using Federal procurement policies to expand the market for secure products, are all good motivations for adopting these proposed mandates.

Personnel Authorities

Because we recognize how difficult it is to recruit the most talented cybersecurity professionals, we support the expanded authorities articulated in this section. We particularly support reactivating and streamlining the program for exchanging public sector and private sector experts.

Data Center Locations

Consistent with our view of financial services as a National market, we support the presumption that data centers should be allowed to serve multiple geographies. We encourage Congress to consider extending this logic for interstate data centers to the international level, while recognizing that the owners, operators, and clients of specific facilities and cloud networks must continue to be held accountable for their security, resiliency, and recoverability of customer data, regardless of the servers' geographic location or dispersion.

H.R. 174

We share the overall objective of H.R. 174, the Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, and we support many of its specific provisions. Listed below are a few comments and questions that we commend to the committee as it considers this bill and the overall issue of cybersecurity policy.

By establishing an Office of Cybersecurity and Communications within DHS, and vesting it with the authority to establish and enforce requirements across sectors, the bill provides for the comprehensive treatment of cybersecurity that we have en-

dorsed above. It offers two options for enlisting sector-specific agencies and primary regulatory authorities in the effort:

Delegation of authorities and responsibilities.—The Director of the Office is given the option to delegate authority to the sector-specific agencies and authorities. We think it is appropriate to invest the Director with this option, much as the administration's proposal has invested it in the Secretary of the Department of Homeland Security and the Director of the Office of Management and Budget.

However, given the inherent uncertainties in how this option might be exercised, we do not believe this should be the sole mechanism for employing sector-specific expertise and authority.

Oversight through sector-specific agencies and authorities.—Throughout the bill, DHS is instructed to consult with its sector-specific partners, have private entities submit information to them, and operate under their guidance. This approach—with DHS setting ecosystem-level standards and sector partners applying them as intermediaries—will reduce the confusion and fragmentation that otherwise could occur in a dual reporting system. We believe that financial institutions will prefer to have their primary regulators continue to serve as their direct supervisor on these issues, even if the Congress determines that some requirements warrant standardization. We believe that this approach merits consideration, along with the standard-with-exceptions and autonomy-with-aggregation approaches discussed in connection with the administration's proposal.

We appreciate the bill's focus on risk-based, performance-based regulations, rather than prescribed measures. As more detail is developed around this approach, at both the legislative and regulatory stages, we believe it may obviate any need for the more prescriptive International Organization for Standardization and the International Electrotechnical Commission standard 15408 (ISO/IEC 15408).

We appreciate the bill's commitment to sharing relevant information to the maximum extent possible, and its designation of private-sector submissions as sensitive security information requiring commensurate safeguards. If other Federal Authorities are actively involved in this process—consulting on threats, vulnerabilities, and consequences, or as members of the interagency working group—we ask that the same information-sharing objectives and protections apply. As the central Department in this process, we see DHS as providing a very valuable contribution by aggregating, analyzing, and disseminating this cross-sector information. We encourage the committee, and ultimately DHS, to leverage the ISACs as a key channel for these communications. We also view research and development as a high value-added opportunity, and appreciate the bill's attention to this function and enumeration of a potential research agenda.

We think two of the definitions articulated in the bill are particularly important, and therefore warrant close consideration. First, the characterization of Covered Critical Infrastructure as systems and assets diverges from the entity-level approach historically applied in the financial services sector. Whether the systems-and-assets or entity-level approach is selected, we urge the Congress to include in Covered Critical Infrastructure not only the core of the critical infrastructures, but also their mission-critical service providers. In financial services, both the operational reality and the regulatory approach require that oversight and other controls extend well beyond the institution.

Second, because the definition of Cyber Incident drives reporting and response protocols, we see it as a key threshold. The current definition, as an occurrence that jeopardizes security, may be interpreted very broadly and, without further detail, may set reporting and response thresholds lower than necessary.

CONCLUSION

We very much appreciate the committee's interest in the important topic of cybersecurity, and particularly in the role DHS plays in this element of critical infrastructure protection. Because The Financial Services Roundtable is fully committed to enhancing cybersecurity:

- We will continue to strengthen security with our members and partners,
- We will help answer this question of integrating DHS' ecosystem-level program and the financial authorities' sector-specific efforts,
- And we will work to pass and implement the administration's cybersecurity proposal.

Thank you very much for your time. I would be happy to answer any questions you might have.

FINANCIAL SERVICES CYBERSECURITY POLICY RECOMMENDATIONS

FINANCIAL SERVICES SECTOR COORDINATING COUNCIL—APRIL 15, 2011

Policy Approaches the FSSCC Supports

Federal leadership on a National cybersecurity framework, implemented with the active involvement, judgment, and discretion of Treasury and the other sector-specific agencies (SSAs).

Commitment to two-way public/private information-sharing, leveraging the Information Sharing and Analysis Centers (ISACs), the US–CERT, safe harbors, clearances, and confidentiality guarantees. This must include sharing of actionable and timely information.

Support focused efforts to address critical interdependencies such as our sector's reliance on telecommunications, information technology, energy, and transportation sectors. Continue to leverage and expand on existing mechanisms (e.g., NSTAC, NIAC, PCIS).

Involvement of Treasury and other SSAs in cyber emergencies.

Federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement.

Public education and awareness campaigns to promote safe computing practices.

Attention to international collaboration and accountability in law enforcement, standards, and regulation/supervision.

Increased funding of applied research and collaboration with Government research agencies on authentication, access control, identity management, attribution, social engineering, data-centric solutions, and other cybersecurity issues.

Increased funding for law enforcement at the international, National, State, and local levels and enhanced collaboration with financial institutions, service providers, and others that are critical to investigating cyber crimes and creating a better deterrent.

Heightened attention to ICANN and other international internet governance bodies to enhance security and privacy protection.

Strengthening of Government-issued credentials (e.g. birth certificates, driver's licenses, and passports) that serve as foundation documents for private sector identity management systems.

Enhanced supervision of service providers on whom financial institutions depend (e.g. hardware and software providers, carriers, and internet service providers).

Recognize the role of Federal financial regulators in issuing regulations and supervisory guidance on security, privacy protection, business continuity, and vendor management for financial institutions and for many of the largest service providers.

Policy Approaches the FSSCC Opposes

Detailed, static cybersecurity standards defined and maintained by Federal agencies in competition with existing, private, standard-setting organizations.

Establishment of vulnerability, breach, and threat clearinghouses, unless security and confidentiality concerns can be definitively addressed.

Sweeping new authority for Executive Branch to remove access to the internet and other telecommunications networks without clarifying how, when, and to what extent this would be applied to critical infrastructure.

Mr. LUNGREN. I thank you, Mr. Williams.

Now Mr. Clinton.

STATEMENT OF LARRY CLINTON, PRESIDENT, INTERNET SECURITY ALLIANCE

Mr. CLINTON. Thank you, Mr. Chairman, Ms. Clarke, Members of the committee. I appreciate your inviting the Internet Security Alliance to this hearing to examine the administration's legislative proposal.

Since ISA represents primarily companies that represent critical infrastructure, I am going to confine my remarks to the regulatory aspects and proposals in the administration's plan.

The Internet Security Alliance is a multi-sector trade organization focused exclusively on cybersecurity. We were formed in 2000. That is nearly 2 years before the events of 9/11, 4 years before DHS was created, 6 years before DHS created a cyber assistant

secretary, 7 years before they filled that position, 9 years before the President appointed a cyber czar, and 11 years before the President sent a legislative proposal on cybersecurity to the Congress. For more than a decade, the private sector has been leading the fight to improve cyberspace.

During this time, we have testified several times before Congress, constantly urging, even begging, Congress and the administration to take a more active role in addressing our cyber threat. There may be some in the private sector who think that the Government should take a hands-off role in this regard. ISA is not among them.

As the Chairman pointed out, the ISA has proposed its own market-based system for improving our cybersecurity system, the "Cyber Security Social Contract," which was cited early and often in the President's Cyberspace Policy Review. We are not alone. Earlier this year, several of the major organizations that represent industry in this space—BSA, CDT, TechAmerica, Chamber of Commerce, and the ISA—banded together to present a detailed white paper of policy proposals for improving our Nation's cybersecurity.

With regard to the administration's position, we find the proposal is both too broad and too Government-centric. Although it has been suggested that the intent of the administration's proposal is to cover core infrastructure, we find a reading of the legislative language rates it as far more extensive.

While there are provisions in the proposal calling for collaboration with industry, we don't need an act of Congress for that sort of collaboration, and the collaboration always ends with Government fiat. For example, Section 7 requires CEOs to certify that they are in compliance with plans required under Section 8 and empowers the Secretary to review any entity's plan. If DHS finds the plan wanting for some reason, they are empowered to, "take any action the Secretary deems appropriate."

In addition, paragraph 4 empowers the Secretary to evaluate the frameworks created through various discussions with the private sector. However, should DHS decide that the standard frameworks don't meet their own criteria, they are empowered to adopt their own criteria and force the companies to choose those.

Government does not have all the answers, and it will not be the best judge of how to manage private systems. Altering our strategy of the public-private partnership to give the Federal Government final say over how private companies manage their systems will be costly, inefficient, and ineffectual.

Moreover, creating this regulatory role for DHS will fundamentally alter the nature of the relationship between Government and the private sector by replacing a voluntary relationship built on collaboration with an adversarial relationship based on regulatory mandates, reports, and compliance. As the research I cite in my written testimony shows, a security system based on that reactive model will be less effective and sustainable.

Now, there is a lot we can do to improve our cybersecurity. As the Chairman pointed out, we need to alter the economic balance with regard to the incentives dealing with cybersecurity. Our testimony, as well as the multi-trade association paper, points out that there is a great deal Congress could do to provide incentives at no

cost to the Government which will lead to the adoption of best practices which a range of studies have indicated can stop between 80 and 94 percent of cyber attacks.

There is another area of cyber attack, many of which Melissa mentioned earlier on, known as the APT, ultra-sophisticated sorts of attack, that are going to require an entirely different strategy. But we do have things in place to deal with that also.

With regard to the administration's proposal, however, we find that the mandatory reporting that they use will diminish motivation for internal investigators, who may worry about finding out material that will be harmful to their company. It will add to the ultimate cost of detection tools and services, making companies more reluctant to spend money on them.

Moreover, we find the evaluation program that is proposed by the administration's proposal to be anti-security. One of the things that everybody agrees on in this space is that we don't have enough cybersecurity professionals. This proposal requires virtually all entities that are covered—and that could be many, many entities—to have annual evaluations. So we are creating an army of insiders roaming throughout the security procedures of our most critical networks on an on-going basis. The value that they would have in terms of providing actual, real security is far offset by the increased risk of having an army of poorly-trained insiders going through our security.

We feel it will be far more preferable for Congress to work with DHS and the rest of the administration to create a system where there are market incentives so that organizations will seek to alter the balance with regard to security return on investment—invest appropriately so that they can have improvements in their own security and our Nation's security.

Thank you.

[The statement of Mr. Clinton follows:]

PREPARED STATEMENT OF LARRY CLINTON

JUNE 24, 2011

I. INTRODUCTION

Good morning Mr. Chairman, and thank you for inviting the Internet Security Alliance to testify before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee.

The Internet Security Alliance is a multi-sector trade association that develops best practices and standards, along with technological, economic, and public policy services focused exclusively on cybersecurity.

ISA was founded and fully funded by a group of private sector entities in 2000. That's nearly 2 years before the tragic events of 9/11, 4 years before Congress created DHS, 6 years before DHS created its first cybersecurity assistant secretary, 7 years before they filled that position, 9 years before the President appointed his first "cyber czar" and 11 years before the President presented his first set of legislative proposals on cybersecurity to the Congress.

For more than a decade, the private sector has been taking a leadership role in the fight to secure cyber space. That is one reason we were delighted when President Obama addressed this issue from the White House and published the Cyberspace Policy Review shortly after taking office—an enlightened document based on an extensive and wide-ranging study by staff of the National Security Council.

II. THE PRIVATE SECTOR HAS BEEN AGGRESSIVELY ATTEMPTING TO UTILIZE THE PUBLIC-PRIVATE PARTNERSHIP TO ENHANCE OUR CYBERSECURITY

Over the past decade, ISA has testified approximately a dozen times before various Congressional committees constantly urging, even pleading, for the Government to take more aggressive steps to enhance our Nation's cybersecurity. There may be some in the private sector that have suggested a hands-off role for the Government in this space, but ISA is not one of them.

And, we are not alone. When legislation began heating up in the last Congress we heard reports from policymakers that there were so many private-sector entities that were interested in the subject that is was becoming difficult for our Government partners to achieve clarity as to where the private sector stood on the issue.

As a result, several of the major associations involved in this debate banded together and worked over a period of 6 months to create a detailed—26-page—white paper specifying our overall approach to cybersecurity and providing detailed policy recommendations.

This unique coalition, which included the Internet Security Alliance, the Business Software Alliance, the Center for Democracy and Technology, Tech America and the U.S. Chamber of Commerce is noteworthy for several reasons.

First, is the obvious size of the coalition, covering literally tens of thousands of companies. Second, is the breadth of the coalition. In the cybersecurity field, the "partisan divide" is generally between the providers of technology and the users of technology. This coalition included both. In addition, the civil liberties community is represented by the most active such organization in this space, CDT.

Finally, there is the depth of the coalition. It is not uncommon to see a coalition of this size in the District of Columbia; however, they are usually brought together on a 1- or 2-page letter. In this case, we have produced an extended, and we think a cutting-edge, detailed policy paper that analyzes a wide range of issues in the cybersecurity space and proposes specific policies—not just broad principles.

Moreover, we sought, as much as possible to be open with our Government partners. We took as our starting points the official publications produced by our Government partners: the National Infrastructure Protection Plan (NIPP) and the Cyberspace Policy Review released by President Obama in May of 2009. Central to both these documents is the need for the Government to work in partnership with the private sector.

This realization has nothing to do with politics. It is based on the fact that in cyber conflicts, it is the private sector that is most likely to be on the front lines and it is the networks owned and operated by the private sector that provide the critical infrastructure—both the regulated and non-regulated ones—upon which any modern nation relies.

Government does not have all the answers and often will not be the best judge of how to manage private systems. Altering our strategy to give the Federal Government final say over how private companies manage their systems will be costly, inefficient, and ineffectual. Cybersecurity must be achieved through a true partnership between the public and private sectors. We specifically endorsed this foundation as embraced in these documents:

"The current critical infrastructure protection partnership is sound, the framework is widely accepted, and the construct is one in which both Government and industry are heavily invested. The current partnership model has accomplished a great deal. However, an effective and sustainable system of cybersecurity requires a fuller implementation of the voluntary industry-government partnership originally described in the NIPP. Abandoning the core tenets of the model in favor of a more Government-centric set of mandates would be counterproductive to both our economic and National security. Rather than creating a new mechanism to accommodate the public-private partnership, Government and industry need to continue to develop and enhance the existing one."[1]

In an attempt to develop our own policy proposals via the established partnership model, we not only notified the White House of our intent to create the industry White Paper, but reached out to them on a regular basis to keep them informed of our progress. We discussed the work at the forums established under the NIPP, such as the IT Sector Coordinating Council meetings, which are regularly attended by DHS staff. When the paper was completed, well prior to release, we sent a full copy to the White House for their review and comment. We requested, and eventu-

[1] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper;* March 2011.

ally received, a 1-hour meeting at the White House to brief them on our proposals and requested on-going interaction so that we could, as partners, come to a common ground on the way forward. Unfortunately, no subsequent meetings were scheduled and we were never briefed on the White House's own—substantially different—approach until it was released and sent to the Congress.

III. WE HAVE THE TOOLS TO STOP BASIC ATTACKS

The committee is aware of numerous and varied cyber attacks. Indeed the internet is under attack all day, every day, and while we successfully deal with the vast majority of the attacks, we also must aggressively improve our cybersecurity.

However, not all attacks are the same. Cyber attacks can of course be segmented many ways, but given the shortage of time, we can create two broad categories; one of basic attacks (which can be extremely damaging) and one of very sophisticated attacks.

Most cyber attacks fall into the first—the basic—category. Although these attacks can be devastating from many different perspectives, they also are largely preventable.

Several different sources including Government, industry, and independent evaluators have concluded that the vast majority of these attacks—between 80% and 90%—could be prevented or successfully mitigated simply by adopting best practices and standards that already exist. Among the sources who have reported this finding we can list the CIA, the NSA, PricewaterhouseCoopers, and CIO Magazine.

Most recently, a comprehensive study jointly conducted by the U.S. Secret Service and Verizon included a forensic analysis of hundreds of breaches and literally thousands of data points and concluded that 94% of these, otherwise successful, cyber attacks could have been successful managed simply by employing existing standards and practices.

IV. WHY ARE WE NOT STOPPING THE BASIC ATTACKS?

Cost.

Some have suggested that the market has failed to produce the needed technology to address the cyber threat. That is not the case.

President Obama's own Cyberspace Policy Review documents the fact that the private sector has developed many adequate mechanisms to address our cyber insecurity but they are not being deployed: "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."[2]

This finding is substantiated by multiple independent surveys that also identified cost as the biggest barrier to deploying effective cybersecurity solutions. This research shows that although many enterprises are investing heavily in cybersecurity, many others, largely due to the economic downturn, are reducing their cybersecurity investments.[3]

The fact is that many companies don't see an adequate ROI to cyber investments. This real-world problem cannot be permanently wiped away by granting a Government department the power to mandate uneconomic expenditures as President Obama himself pointed out last year at the White House: "Due to the interconnected nature of the system this lack of uniform implementation of sound security practices both undermines critical infrastructure and makes using traditional regulatory mechanisms difficult to achieve security."[4]

Rather, we need to find ways to work within the partnership to encourage firms to make investments that may go beyond their own commercial risk management requirements for security, but might rise to the level of a broader National interest. This principle was recognized in the creation of the original NIPP:

"The success of the [public-private] partnership depends on articulating the mutual benefits to Government and private sector partners. While articulating the value proposition to the Government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector . . . In assessing the value proposition for the private sector, there is a clear National security and homeland security interest in ensuring the collective protection of the Nation's [critical infrastructure and key resources] (CI/KR). Government can encourage industry to

[2] Obama administration, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31.

[3] PricewaterhouseCoopers, *The Global State of Information Security,* 2008. Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* 2010.

[4] White House, *Remarks by President Obama at White House Meeting on Cyber Security,* July, 2010.

go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activities such as:

- "Providing owners and operators timely, analytical, accurate, and useful information . . .
- "Ensuring industry is engaged as early as possible in the development of initiatives and policies related to [the NIPP].
- "Articulating to corporate leaders . . . both the business and National security benefits of investing in security measures that exceed their business case.
- "Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices.
- "Providing support for research needed to enhance future CI/KR protection efforts."[5]

The Obama "Cyberspace Policy Review" went even further in suggesting this pathway by suggesting a mix of tailored incentives including liability incentives, procurement incentives, indemnification, and even tax incentives.

The multi-trade association White Paper continued this chorus of support for this approach.

"One of the most immediate, pragmatic, and effective steps that the Government could take to improve our Nation's cybersecurity would be to implement the recommendations made in the CSPR to explore incentives, such as liability considerations, indemnification, and tax incentives. For example:

- "Tax incentives that encourage establishing additional cybersecurity investments, such as the R&D tax credit;
- "Grant funding is used effectively in other homeland security areas such as emergency preparedness and response. Critical infrastructure industries can use grant funds for research and development, to purchase equipment, and to train personnel;
- "Streamlining regulatory procedures, which would cut both Government and industry costs;
- "Updating the SAFETY Act to better appreciate the cyber threat that has become more evident since its enactment. This Act, which provides a mix of marketing, insurance, and liability benefits for technologies designated or certified by DHS, can be expanded to standards and practices as well as technologies that protect against commercial as well as terrorist threats;
- "Liability protections or regulatory obligations (e.g., for utilities) adjusting in numerous ways to provide incentives for enhanced security practices, such as adoption of standards and practices beyond what is required to meet commercial risks, or enhanced information sharing. Liability benefits do not need to be elevated to immunity to be attractive. Categories of liability (e.g., punitive vs. actual damages) or burden of proof levels (preponderance rather than clear and convincing evidence) can be adjusted to motivate pro-security behavior without costing taxpayer dollars; and
- "Stimulating the growth of a private cyber insurance industry that can both provide private economic incentives to spur greater cybersecurity efforts while also creating a private market mechanism that fosters adoption and compliance. The Government should give consideration to implementing reinsurance programs to help underwrite the development of cybersecurity insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gain experience with cybersecurity coverage.

To accommodate the needs of a wide variety of critical infrastructures with different economic models, the public-private partnership should develop a menu of incentives that can be tied to voluntary adoption of widely-accepted and proven-successful security best practices, standards, and technologies. The R&D tax credit may be the most attractive option for an IT security vendor, while a defense firm may be more interested in procurement options, an electric utility in a streamlined regulatory environment, or an IT-user enterprise in an insurance discount and risk transfer. Many of these incentives are deployed successfully in other areas of the economy, but not yet to cybersecurity."[6]

V. ADDRESSING SOPHISTICATED ATTACKS

While most cyber attacks are fairly basic and can be stopped or mitigated with the deployment of existing standards, practices, and technologies which could be

---

[5] *National Infrastructure Protection Plan,* 2006 at 9.

[6] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity Through the Public-Private Partnership: A White Paper;* March 2011 at 10–11.

achieved through the use of a creative incentive system, there are still other much more insidious and sophisticated attacks that are not going to be stopped with best practices.

Again, there are many ways to characterize these attacks but one common term that has come to be used somewhat generically in the field is the Advanced Persistent Threat (APT).

Without getting into the academic debate over what constitutes the APT, it suffices to say these are sophisticated attacks. These are not "hacker kids" or kids in basements. These attacks are formulated by highly sophisticated, well-organized, well-funded, often state-sponsored attackers. These guys are pros. They are very good, and if they target you or your system you can be pretty sure they will succeed in penetrating, or "breaching" your system.

However, this does not mean we have no defense. Indeed, many companies have been working for several years with some success on mitigating APT attacks although it necessitates altering our defensive posture from one of perimeter defense geared to stopping breaches to internal detection and mitigation.

Again, the private sector White Paper identifies some of the current core strategies that the Government, in collaboration with the private sector ought to be deploying to address the APT style (ie. more sophisticated) attacks. However, it is important to note that there is no silver bullet to addressing these advanced threats.

The core reason we have attacks, and they will likely continue, is that the economic incentives generally favor the attackers. Many attacks are cheap, easy, and profitable while on the other hand, an infinite perimeter needs defending, it is very hard to catch and prosecute cyber attackers and it is difficult to demonstrate ROI to things that you have prevented such as cyber attacks.

So long as our economic equation for cybersecurity remains out of balance, we are going to continue to have attacks. This needs to be understood not as a discrete problem for which there will be a simple and unchanging security technology—like a seat belt or a set of gold standard Government metrics. Rather, this is an on-going and persistent threat that needs continuous deployment of creative strategies that evolve with the dynamic threat.

VI. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL

Unfortunately, after waiting 2 years for the administration to follow up on its CSPR, we received a legislative proposal produced without coordination with the private-sector partnership the administration itself had established for this purpose, and which:

- Fails to follow up on the promise of earlier work by this and the previous administration;
- Does not address the core economics issues which drive our lack of cyber insecurity;
- Would create an extensive new bureaucracy that will not address the persistent cyber threats we face; and
- Could add significant new threats that are not justified by the dubious benefits of the unbounded intrusions into our most critical infrastructure.

Since ISA works primarily with major entities from most for our Nation's critical infrastructure, we will focus our testimony to Section 3 of the President's proposal, which establishes a new and extensive regulatory structure over the private sector.

VII. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL FUNDAMENTALLY ALTERS THE PUBLIC-PRIVATE PARTNERSHIP

When he released the Cyberspace Policy Review in 2009 President Obama himself said:

"Let me be very clear: My administration will not dictate security standards for private companies. On the contrary we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."[7]

Unlike the rigorous and open process the Obama administration conducted in developing the Cyberspace Policy Review, the current legislative proposal was not developed in any way by "collaboration with industry to find technology solutions."

ISA participates in numerous bodies set up under the NIPP to facilitate this sort of coordination including the Sector Coordinating Councils, the Cross Sector Cybersecurity Working Group, the Critical Infrastructure Partnership Advisory Council (CIPAC) and the Software Assurance Forum. Despite repeated requests for the administration to engage with these bodies, designated by them for collaboration to develop solutions, there were no discussions at even a conceptual level about this

[7] President Barack Obama, Release of the *Cyberspace Policy Review,* May 29, 2009.

proposal which would, if enacted, fundamentally alter the long-standing relationship.

Had the administration used the bodies designated for this sort of interaction, I believe the proposal would be both substantively stronger and politically more practical.

Notwithstanding the process, the Centerpiece of the proposal—the establishment of an unbounded regulatory structured for the Department of Homeland Security—is obviously directly at odds with what the President pledged when he released the Cyberspace Policy Review 2 years ago.

Obviously it will be the the committee and the Congress' decision whether to follow this new Government-centric approach, but there should be clarity at the very least that by establishing a broad regulatory framework, as this proposal does, it will fundamentally alter the nature of the relationship between the Government and private sector.

It's often said that to a hammer, everything looks like a nail. And prisoners and prison guards do not have a partnership. One body is mandated to do what the other entity directs. While there is a fair amount of verbiage in the administration's proposal about working with the private sector, as we will discuss shortly, at the end of the day, this legislative proposal will allow DHS to regulate pretty much any entity it elects to regulate and mandate whatever DHS elects ought to be mandated.

Some may argue that such a system of regulatory mandates will finally solve our cybersecurity problem; however, there is no evidence that this will be the case. Indeed, the academic research on motivating investment in information security specifically points in the opposite direction indicating that "proactive" investments motivated by market incentives are more effective than reactive (prompted by regulation) are.

A new study released from Dartmouth College earlier this month documents this finding, "Proactive investments are more effective at reducing security failures than reactive investments. When proactive investments are forced by an external requirement, the effect of the proactive investment is diminished . . . our results show that learning by doing through proactive security investments relies on economic incentives whereas unilaterally mandated procedures do not have any economic incentive . . . Government requirements simply focus attention on the problem area rather than discovery and learning by doing . . . external pressure does not have significant social incentives."[8]

VIII. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL IS NOT SUPPORTED BY RESEARCH OR PRECEDENT

Research[9] has consistently shown that the single biggest barrier to enhancing the cybersecurity of our Nation's critical infrastructure is economic. As previously mentioned, the National Infrastructure Protection Plan (NIPP)[10] identified the need for Government to create a value proposition for industry to make investments in cybersecurity that are not justified by their business needs, but may be required for overall National security. In fact, the Cyberspace Policy Review specifically advocated the development of proactive market incentives such as procurement, tax, and liability to incentivize additional cybersecurity investments.[11]

However, the administration's legislative proposal does not follow through on any of these policy commitments.

Instead the administration's current legislative proposal relies primarily on "disclosure" as a market incentive, to hoping that reaction to such a public disclosure will generate increased cybersecurity investment. While at one point this may have made sense, it is not likely to be helpful when addressing the current attacks we face.

IX. THE FOCUS ON DISCLOSURE OF BREACHES IS OUTDATED

Most cyber attack disclosure requirements are founded on misconceptions about what it is companies have available to disclose. Most successful modern cyber attacks go undetected. Furthermore, cyber intrusions and malware, as they become more sophisticated and more damaging, become increasingly difficult to detect. The

---

[8] Kwon, Juhee, and Johnson, Eric; *An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security.* Dartmouth College, NH. June 2011 at 18.

[9] PricewaterhouseCoopers, *The Global State of Information Security,* 2008. Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* 2010.

[10] *The National Infrastructure Protection Plan* (NIPP) is available at *http://www.dhs.gov/files/programs/editorial_0827.shtm#0.*

[11] Executive Office of the President, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure,* May 2009.

tools and services for detecting them are very expensive, and the evidence for their presence is often very ambiguous.

The fact that the proposed legislation and the discussions that surround it are constantly referring to "breaches" shows how rapidly policy in this field becomes dated. "Breaches" were the big cybersecurity concern of the last few years, but they are not the big cybersecurity concern of the era that began with Stuxnet. What's more, the very term "breaches" suggests that the remedy to cyber attacks is perimeter defense—guarding the organization's information border against forces attempting to penetrate, or "breach" it. This is a way of thinking about cybersecurity that many of the foremost cybersecurity experts have been arguing is obsolete for half-dozen years now. ISA presented this finding to the Obama administration which cited the study in their Cyberspace Policy Review and published it on the White House website, but did not reference it in their own legislative proposal.

In fact, most companies are unable to tell whether they have been the victim of a successful cyber attack unless they make a special effort to investigate, spend additional resources on the effort, and have the necessary skills and tools already on hand. The initial signs that need to be pursued in order to discover a skilled cyber attack are hard to define, constantly changing, and often very subtle and thus unsuitable for the annual evaluation procedure the administration proposes to rely on. Uncovering a highly-skilled cyber attack is currently much more of an art than a science. It can require intuition, creativity, and a very high degree of motivation.

X. THE ADMINISTRATION'S PROPOSAL CREATES THE WRONG INCENTIVES

Mandatory disclosure punishes companies that are good at detecting intrusions and malware. It creates an incentive not to know, so that there is no obligation to report. It diminishes the motivation of internal investigators, who may worry that finding out exactly what happened may do their company more harm than good. It adds to the ultimate costs of detection tools and services, making companies more reluctant to spend money on them.

Requiring companies to disclose their cybersecurity plans and certifications is, if anything, even more likely to have unintended consequences than requiring disclosures of successful cyber attacks. The kinds of language and administrative formulas that would be adopted to comply with such requirements would almost certainly have little to do with real cybersecurity. This is partly because the field is developing so rapidly that by the time cybersecurity plans were recognized as fulfilling administrative expectations, they would already be obsolete. There is also no way to tell at the level of a "general plan" whether the cybersecurity measures involved would be doing any good or not. The consequence of disclosing such plans would be another, costly level of administrative bureaucracy and auditors that would probably only be getting it the way of good security.

XI. ADMINISTRATION'S PROPOSED LANGUAGE PROVIDES DHS WITH UNFETTERED AND UNJUSTIFIED AUTHORITY OVER PRIVATE SYSTEMS

Although it has been suggested that the intent of this legislation is to cover only the most critical "core" infrastructure, a careful reading of the legislative language indicates that it provides essentially unfettered authority to DHS to mandate technical standards for almost any aspect of the private sector.

Sec. 3 of the Regulatory Framework for Covered Critical Infrastructure lists a full page of requirements to be met before an entity is subject to these, as yet unspecified, Federal mandates.

However, when reading through them, they don't provide any limit on the Secretary's authority to designate any enterprise as a so-called "covered critical infrastructure" and thus subject to DHS mandates.

It's easiest to analyze the impact of the sections if we review them in reverse order.

Subsection D states that being named on the list as a covered critical infrastructure under this section "shall be considered a final action for purposes of judicial review."

Subsection C lists a variety of criteria to be placed on a "risk-based tier," but criteria No. 4 is "such other factors as the Secretary deems appropriate," which means the Secretary can place any entity on any tier for any reason he or she wants to.

Subsection B, which lists only 2 criteria for inclusion. One criterion is that the entity or system "is dependent on information infrastructure to operate."

Since virtually all modern systems that are reliant on some form of information infrastructure to operate, those criteria are all-encompassing.

That leaves us only with the criteria listed section B1, which is that incapacity or disruption of the reliable operation of the system would have a "debilitating effect on National security, National economy, or National public health or safety."

We regard "debilitating" as a fairly loose, and frankly weak, criterion for conferring such broad authority to the Secretary. To "debilitate" simply means to weaken—it doesn't necessarily mean to weaken a lot—just weaken. When I catch a cold I'm somewhat debilitated—but I wouldn't want the CDC to have the power to therefore regulate me.

According to this legislative language, if the Secretary decides, for any reason, that the incapacity of a system might in some way weaken our economy, security, or safety, he or she has the authority to mandate—as a final action—whatever technical standards over their cyber systems the Secretary desires.

For example, the recent SONY Play Station attacks reportedly will cost more than a billion dollars in damage, which one can argue weakens or "debilitates" the economy at least somewhat. Would that then make SONY Play Station's "covered critical infrastructures" under this definition? When asked that question at a recent Judiciary Committee hearing, an administrative witness replied that that determination would have to be made through rulemaking under the Act.

In addition, the language does not state that the debilitating effect referred to in Sec. (b)(1) has to be from a cyber incident. According to this legislative language, the fact that the World Trade Center was attacked with airplanes, which obviously had a debilitating effect on our security and economy, would be justification for DHS to impose mandates on the cyber systems operating in the WTC, even though they had nothing to do with the attack.

In addition, one criteria DHS will use in assigning an entity as a covered critical infrastructure is its interconnectedness with other infrastructures. That again allows for a tremendous expansion of potential DHS authority.

For example, the supply chain for weapons systems can be thousands of companies long. Obviously, interruption of the operation of these systems for whatever reason—including non-cyber reasons—affect our National security. So under this language, all these thousands of other companies would be potentially subject to DHS regulation due to their interconnection to the main weapons system project.

Moreover, under Sec. B1 of this provision, DHS will regulate "entities" as opposed to systems or assets. This presumably means that an attack having a debilitating—however minor—effect on security, economy, or health would result in the regulation of the entire entity the system is interconnected with.

The bottom line is that this legislative proposal provides almost unbounded discretion for DHS to classify an entity as covered critical infrastructure and subject the entire entity to unspecified regulation.

Section 9 states specifically that "the Secretary shall promulgate regulations . . . to carry out the provisions of the Title."

Section 2 states clearly that one of the purposes of the Act is to "establish workable frameworks for implementing cybersecurity minimum standards and practices."

Some may ask, "what's wrong with DHS establishing minimum standards for industry through a rulemaking." The problem is it won't work and it is substantially counterproductive.

Now, ISA is a big fan of standards and practices and we work with many entities, including NIST and other Federal Government agencies as well as private sector entities to create and constantly update them.

However, there is a major difference between using the existing consensus process to develop international standards and practices and having a Government entity determine such standards and mandate them on the private sector.

The multi-trade association White Paper addresses this argument in an entire section, concluding that:

"[w]e have already seen that attempts to impose Nation-specific requirements under the auspices of security are not embraced by the private sector or the civil liberties and human rights community for both public policy and economic reasons. A Government-controlled system of standards development that resides outside the existing global regime will not be accepted. If imposed, it would quickly become a second-tier system without widespread user or technology community adoption, thereby fracturing the global network of networks and weakening its security."[12]

[12] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity Through the Public-Private Partnership: A White Paper;* March 2011 at p. 8.

Again, although there is a great deal of verbiage discussing how the Government will work with the private sector, the bottom line is that this legislative proposal consistently gives DHS massive new regulatory authority.

Section 7 requires CEOs to certify that they are in compliance with the plans required under the Act. Although there is substantial verbiage suggesting that DHS will work with the covered entities in creating these plans, Section 8 empowers the Secretary to review any entity's plan, and if DHS finds the plan wanting for some reason, they are empowered to "take such action as the Secretary deems appropriate." In addition, paragraph 4 empowers the Secretary to evaluate the frameworks created through various discussions with the private sector. However, should DHS determine that the standardized frameworks don't meet their criteria, they are empowered to adopt their own framework to meet their criteria, and, thus, the DHS framework would be what a covered entity would be required to implement and certify.

XII. THE ADMINISTRATION'S PROPOSAL FOR EVALUATION IS ANTI-SECURITY

Under this proposal, an apparently enormous range of companies would be required to construct plans for cybersecurity and plans and be required to hire Federally-approved "evaluators" to review their internal security on an annual basis. There is little if any evidence that regulatory compliance is per se improved security. Indeed, many report that compliance requirements distract personnel from security work to attend to the compliance regime.

Moreover, it is acknowledged on all sides that we face a critical shortage of qualified cybersecurity personnel and so the army of evaluators created under this proposal will almost by definition not be adequately trained.

The single largest vulnerability of our cyber systems comes not from hackers using technology to break into systems but from "insiders" with approved access to the systems. This proposal creates a virtual army of insiders crawling through our most critical infrastructure's security systems on an annual basis.

The threat of introducing constant stream of new "insiders" into our Nation's most critical infrastructure far outweighs the dubious assumption that they will provide a tangible security benefit. That does not even account for the costs industry will bear to hire these evaluators, the cost of new manpower at DHS to comb through this mountain of data and the potential of an ideal attack vector where all these reports detailing our Nation's security will be stored.

XIII. THE INFORMATION GENERATED BY THESE DISCLOSURES WON'T ENHANCE SECURITY

Ironically, one of the unintended effects of more comprehensive or stringent disclosure laws could be less information about the sort of cyber attacks that really matter. This is because most of the mandated disclosures would simply be noise. There would be a constant stream of reports, based on what lawyers believe would demonstrate compliance, while actually revealing as little as possible. This stream of reports would obscure the attack trends that really matter, while allowing companies to conceal events that might otherwise provoke public outcry and more active Government intervention. As cyber attack disclosures have become more frequent and more routine, this has already been already happening.

The information made public by disclosure requirements is usually not very meaningful. Most cyber attacks, even if they are successful, do relatively little harm. They gather information that the attackers are never able to utilize. They provide one component of a larger attack program that never comes to fruition. In many cases, the effects of the disclosure are considerably worse than the effects of the attack itself. The mere fact that a company has suffered a successful attack gives little indication of its actual losses, even if specific numbers are mentioned. This is because there are so many factors that can influence the scale of loss, including the wording of the disclosure itself. Determining how much a successful cyber attack will hurt a company is very difficult even for those who have access to all of the details of the attack, the operations affected, and the company's finances. For the general public, the bare facts of a successful cyber attack are often very misleading.

The cumulative data from the cyber attacks that have so far been publicly reported are also very misleading. Many of the biggest reported losses of personal data were due to lost or stolen laptops. This is not because it is the main way personal data is stolen; it is because the loss or theft of a laptop is an unambiguous event that it is hard not to acknowledge. Many of the other reported losses of data have been from major defense contractors. This is not because the major defense contractors are losing more data than other companies or than Government departments; it is because they have the best detection systems in place. Some of the most publicized cyber attacks have involved Google mail. This is not because Google mail has

been compromised more than other e-mail systems; it is because Google's business model depends more on trust and on certain types of transparency than the business models of the other companies providing e-mail services. Since most cyber attacks go unrecognized, the mere fact that a cyber attack is being reported means that it is atypical.

XIV. USING EFFECTIVE MODELS (A) THE CDC

All of this does not mean that all disclosure laws or bad or even that the existing ones are bad. It merely points out the unintended effects of such laws that legislators need to make an effort to avoid in drafting additional laws. More information about cyber attacks in general and about the degree to which individual systems and companies are at risk is necessary for markets to take adequate account of these things. Disclosure laws could provide some considerable benefits. But they will not provide the intended benefits unless they take into account how systems are monitored for attacks and what additional information might be needed to put the attacks in context.

It is possible that the best approach might be to have the reporting go to a special legislatively-created institution, rather than directly to the public. This is the model used with disease control and public health issues. With sufficiently clear instructions as to how this institution would handle the information, its actions could potentially be accepted by all parties. There are other ways disclosure could be handled that would be less crude in its effects. The point here is that any disclosure laws need to be framed with a conscious acknowledgment of the pitfalls.

XV. EFFECTIVE MODEL (B) SEMATECH

In the 1980s, the United States also faced a technological onslaught. During this decade, the nation of Japan began flooding the U.S. market with computer chips, which threatened to drive U.S. chip manufacturers out of business. Recognizing the economic and security threat that this posed, the U.S. enacted legal measures such as the Federal R&D tax credit and the Cooperative Research Act of 1984, which eventually led to the private sector and U.S. Department of Defense cooperative known as SemaTech. Within 2 years, sub-micron architectures, advanced X-ray lithography and a number of other critical innovations pushed U.S. chip makers back into world leadership, and produced generation jumps in computing capabilities just as the internet was dawning.

A similar Cybersecurity Public-Private Cooperative could be composed of the private sector, academia, and the Government in a minority role. This organization could be charged with improving, even reinventing the cyber ecosystem in a more secure manner. Under this Cooperative's umbrella, stakeholders could share information and cybersecurity technology development to create (or fund the creation of) more alternative networking protocols, software languages, and/or hardware architectures that are more secure. It could also act as an incubator for ideas to create better strategies to combat APT's and their equivalent. It could also serve as the equivalent of an underwriters laboratory for cybersecurity by independently assessing best practices and standards along sliding scales. These proven increasing levels of security, if voluntarily adopted, could then be used to qualify enterprises for subscribing to them in return for the incentive programs suggested earlier which will help mitigate costs while enhancing proven security practices.

The ISA, its members and partners are aware of the need to combat cyber threats—indeed that is why ISA was created over a decade ago. However this must be done in collaboration with Government, not as mandated by Government. Moreover, the solutions we derive must be both technologically and economically practical if they are to have the sustainable effect we require.

Mr. LUNGREN. Thank you very much, Mr. Clinton.

We will now go to a round of questions, 5 minutes for each Member, and I will begin.

Ms. Hathaway, you heard Mr. Clinton's forceful testimony there. How do you respond to that?

Let me just give a little background. I have said as a general rule what I would like to do is to ensure that we have a cooperative spirit between the private sector and the public sector, No. 1. No. 2, my concern is, if we are not deft enough in the way we have our regulatory schematic, we could—not intended to do this—but we could have the result of stifling creative ways of protecting against

cyber attack that might come from the private sector as we impose a Government one-size-fits-all approach.

So I would like to see us, I guess, hit the sweet spot in that. You have been there, you have been through these arguments, and helped set up the contours of the debate. How do you respond to Mr. Clinton's observation about the administration's proposal?

Ms. HATHAWAY. Sir, I think that the administration's proposal had the opportunity to engage the private sector to inform the debate and the items within the proposal. But during the course of their review, they did not engage the private sector, which is why it is so important that this committee and other committees do engage the private sector in understanding what are the second- and third-order effects of regulation and other market levers.

I think it will be important to take a look at both a regulatory framework and an incentives-based framework for research and development, for incentivizing industry to actually get to a standard of care where we are not actually seeing breaches on a regular basis.

Mr. LUNGREN. One of the concerns that I have had expressed to me by some in the private sector—others have indicated very strong support for the overall proposal—but one of the areas of concern was the auditing aspect contained in the proposal, where some suggested it was overreach.

Now, Mr. Clinton, you suggested this sort of a continual presence there might open up the possibility of security breaches that wouldn't otherwise exist. I suppose that is always a balance you have to have.

How do you ensure that those that you hope are protecting against cyber attack in the private sector, with consequences to individuals on a more general basis, how do you ensure that that is being done and, at the same time, don't have a heavy hand, which may result in exposures to intrusions that you otherwise would not have? How do you hit that balance?

Mr. CLINTON. The best way to do it, I believe, Mr. Chairman, is to make the system—to establish the system so that the organizations want to invest in security, so that they see it as in their own self-interest.

As I think was pointed out earlier in some of the opening statements, what we currently have and what the National Infrastructure Protection Plan says is that we have not currently recognized the value proposition for industry. In some industries, there may not be an adequate value proposition. But there are a variety of ways that we can alter that so that they want to invest more in cybersecurity, they see a benefit to it.

One way——

Mr. LUNGREN. So they can explain to their shareholders or justify to their shareholders and their board of directors that it is bottom-line-effective.

Mr. CLINTON. Sure. One of the ways I think you mentioned in your opening statement is through the use of insurance. We have not been done enough to bring the insurance industry into the cybersecurity equation. Insurance is one of the great drivers of prosocial behavior. We use it in health care. We use it in—my daughter drives more carefully because she wants a "good driver" dis-

count on her insurances. This affects things. But we have not brought insurance into the cybersecurity arena.

If we were able to motivate the greater adoption of insurance, the insurance companies will do the evaluation for us because their money is at risk. We can also use the reductions in premiums to provide a motivation for the adoption of increased best practices, just as we do when people give up smoking to have lower insurance rates, et cetera, et cetera.

Insurance, liability reform, better use of procurement, which has already been mentioned, streamlined regulation—these are all things that could be offered to the private sector in return for investing more in cybersecurity that will adhere to their bottom line, making it so they want to do it, not because we are making them do it, and at the same time enhance our own Nation's cybersecurity.

Mr. LUNGREN. Within the administration's proposal is a proposal for a National law on notice of breaches, which would, as I read it, preempt the States from doing that and, therefore, alleviate what some would say is a patchwork of different notice requirements. On the other hand, people say States should have the right to do that.

Does anybody on the panel have a disagreement with the administration's approach on that?

All right.

The gentlelady from New Jersey, the Ranking Member of the subcommittee, is recognized.

Ms. CLARKE. I am from New York.

Mr. LUNGREN. Excuse me. New York.

Ms. CLARKE. It is okay. But you know, as a New Yorker, we have to set the record straight.

Mr. LUNGREN. After Mr. Pascrell yesterday indicating that he represented the entire region, I am sorry.

Ms. CLARKE. There you go. There you go.

Let me start with you, Mr. Clinton, and the whole idea of incentivizing and the how-tos. You raised the issue of insurance, and I want to explore that a little bit further. Certainly, incentivizing insurance, on the surface, seems like a proposal that perhaps could work.

What would happen if industry didn't bite or part of industry did but the other part didn't? How do we create sort of a uniform incentive?

Because, you know, some folks could say they want it, and some folks could say, you know what, thanks but no thanks. Then we are still left vulnerable, because if everyone isn't involved, then vulnerabilities will exist.

Can you speak to that?

Mr. CLINTON. Certainly, Ms. Clarke. Thank you very much.

What the ISA proposes and, frankly, what is proposed in the multi-trade association white paper speaks exactly to your point, which is accurate. We have a very diverse private sector. So what we advocate is that we need to develop a menu of incentives.

Certain incentives will be very attractive to certain areas. So, for example, if you are in the defense industrial base, procurement incentives are going to be particularly of interest to you. If you are

in the public utility space, perhaps streamlining some of the regulation to make it more cost-effective may be appropriate to you. Other sectors are going to be interested, perhaps, in insurance. Still others might be interested in liability reform. You have to have a multitude of incentives, because different things will motivate other people.

Were you also asking about how to get the insurance stuff started?

Ms. CLARKE. Well, I think my question is more to, when you deal with things from a voluntary perspective, entities can opt out. With cybersecurity, any opt-out equates to a vulnerability. Any area of penetration can then have a cascading effect. So, you know, while we want to resist the idea of imposing anything, I am just trying to get at, you know, how do we deal with trying to get as much coverage as we possibly can?

I understand the menu that you have discussed. Perhaps it is industry by industry, where we get buy-in through each industry and its leadership, that will then cast the net that we are looking for to close those vulnerabilities.

Would anyone else want to address that issue?

I am just trying to figure out, without imposing a standard, if you will, how do we get everyone to see the virtue in establishing a standard that we can hold everyone accountable for?

Mr. WILLIAMS. Representative Clarke, if I might, I absolutely agree with Mr. Clinton, that we should do everything in our power to set a private-sector leadership model in this, as we have in the past, to rely on markets wherever possible. If the insurance and incentive models work where they work, fantastic.

Our experience in financial services is that, with a combination of regulatory oversight and our own business motivations, we have done a better and better job of protecting our sector. We have also reached out to other sectors with uneven results. So our service providers and the sectors on which we in a very interconnected way always depend are often receptive to their business partners saying, "Security is important; we need you to invest in it," but not always.

That is our concern. That is our motivation for supporting a comprehensive proposal here, is that if some opt out and they don't happen to be in a critical tier, well, that may be perfectly reasonable. But at least for that most critical tier, opt-out and the possibility that at least some business partners will just decide to go their own way and put others at risk we think is problematic.

Ms. CLARKE. Mr. Williams, let me just ask another question. Why do you think that preemption is important? Do you think there is a role for States in cybersecurity policy?

Mr. WILLIAMS. One way to think about the State model, as people often describe it, is that it is a laboratory. In breach notification and in many other areas of cybersecurity and consumer protection, it has been a wonderful laboratory. We have seen these breach-notification rules evolve over the last several years with various experiments in the different States.

We believe that it is now much more mature and that now we are ready for a National model. Those experiments have yielded

the fruit that we would expect, we have some experience now, and we would like to see some uniformity at the National level.

The States may still very well have responsibility for, in our case, overseeing State-chartered institutions like banks and insurers. They may still have consumer protection authority. But cybersecurity we think of as a National issue where uniformity, we think, makes the most sense.

Ms. CLARKE. Thank you very much, Mr. Chairman. I yield back.

Mr. LUNGREN. The gentlelady yields back.

The gentleman from Texas, Mr. McCaul, is recognized for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman.

I think as you point out, Mr. Williams, I agree with the breach-notification law. It really cries out for National Federal law.

There are many things in the administration's proposals that I agree with: The increased penalties for computer hacking; the notification law; the clearer cybersecurity authority for DHS; the FISMA reforms, which I think are necessary. So I would have to say, overall, I think Howard Schmidt, I think, did a pretty good job.

But the one area where I find myself in disagreement really relates to the private sector and what role the Government plays in regulating the private sector. I think the first principle that we have, particularly in this area, in Congress is to do no harm. I think we can legislate and have unintended consequences, particularly as it applies to the private sector.

We can harden the Federal networks, and I think that is something we are very focused on. You know, the Einstein 3—I mean, there are a lot of things in this proposal that deal with that. But it is really hardening the private sector and the critical infrastructures in the private sector that I think are the greatest challenge for us as policymakers. Ninety percent of the critical infrastructures, up to, are really controlled by the private sector.

So my first question is to you, Mr. Clinton. How can we enhance that and incentivize the private sector without having these punitive mandates?

The one thing in this proposal I disagree with is the regulating over the private sector. Then if they are out of—I mean, the remedy for a violation is basically what we call "name and shame." You know, we will call out the company and then publicly call out the vulnerability, which I don't think that is very good policy, to be, you know, publicly showing where a company is vulnerable. That just invites more mischief.

So give me your thoughts on the regulating part of this provision, and what would you recommend?

Mr. CLINTON. Well, certainly, I agree with you, Mr. McCaul, about the disclosure aspects here. It creates a target. Not only that, it creates an incentive for companies not to find out things. You know, we need to incentivize people to be doing a better job of reviewing their cyber systems.

You know, the modern cyber threat is geared around not allowing you to know that it is there. I mean, you know, a few years ago, cyber threats, you know, were—you had big cutesy names like the "Love Bug" and "Blaster" and all that kind of thing. Modern cyber threats are stealthy. They get in your system, and the first

thing they do is clean out your system, so that when there is detection done, none of these lousy cyber threats let you know that the really bad guy is there. They go in your system and they hide. So it is very difficult to find these guys.

So we want to provide incentives for people to go and look at them. If the corporation knows that the harder they look for a problem, the more likely are they are going to be named and shamed for finding it, we have created exactly the wrong incentives.

It would be much better if companies were proactively incented in the way that I suggested with Ms. Clarke so that they wanted to go find these things because they were going to lower their liability, they were going to lower their insurance rate, they were going to have a better chance at a Federal contract, et cetera, et cetera.

The one point that I think we have to be sure, though, is that we don't assume that there is some sort of minimum National standard that everybody has to get to. That is not true. The problem that we have with cybersecurity is not that the technology is broken and so we have to bring it up to standard; the problem with cybersecurity is that it is being attacked from the outside. So we have to find a way to motivate a continual investigation and innovation of mechanisms, rather than bring people up to some sort of stable standard.

Mr. MCCAUL. Thank you.

My time is limited. Ms. Hathaway, I wanted to ask you a quick question. You have a lot of expertise in these public-private partnerships. We have had the ISACs, the information sharing and analysis centers; have never really gotten to the point where we want them to be. You know, when I met with some of these firms in Silicon Valley, they talked about the liability protections. You know, there is a FOIA exemption, or exception, for critical infrastructures in terms of the sharing, but there still isn't any liability protection for them. So they are not incentivized to share information.

Can you speak to that? What would be your recommendation as to how we can better enhance these public-private partnerships?

Ms. HATHAWAY. Representative McCaul, I agree that many companies perceive that the FOIA is not strong enough if it were actually leveraged, and, therefore, private-sector entities are not as willing to share information.

I think that the question we need to be asking ourselves on the Government side is, how can we share more and better information with the private sector so they can appreciate the threat that they are dealing with and the exposure that they have as multinational corporations?

I think the Government does not share actionable information with the private sector and should increase their information-sharing mechanisms that are informed from the law enforcement and the intelligence community.

DHS, as the forward-facing entity, needs better information from the law enforcement and intelligence community and should be sharing actionable information and real case studies with the private sector of what is happening in their industry, how certain cor-

porations are being exposed—not necessarily naming them, but saying company *X* was exposed with the following breach and lost *X* quantity of confidential information. It is only when we start using real cases and real information that the private sector will be able to better defend itself.

Mr. MCCAUL. Thank you, Ms. Hathaway.

Mr. LUNGREN. The gentleman yields back.

The gentleman, Mr. Richmond, is recognized for 5 minutes.

Mr. RICHMOND. I defer to Laura my time. I think she needs to leave.

Mr. LUNGREN. Oh, okay. Well, according to the rules of the committee, it is in order of appearance. So Mr. Keating would be next unless he allows Ms. Richardson——

Ms. RICHARDSON. I think I was here.

Mr. LUNGREN. Okay. The gentlelady from California, Ms. Richardson, is recognized.

Ms. RICHARDSON. Thank you.

Thank you, gentlemen. That was very kind of you.

Ms. Hathaway, in your opinion, which sectors are the most critical that we should be focusing on? We obviously can't do everything. We are not going to have money for everywhere. In our critical infrastructure, what would you say would be most vulnerable?

Ms. HATHAWAY. Ma'am, I think that the most important probably starts with our energy sector. Without the power, you can't run a business and you can't sustain operations. Given the system control vulnerabilities and in the wake of the proliferation of Stuxnet, it is a high priority for the country to address the vulnerabilities that are within the power sector.

I think followed by power is telecommunications, because without telecommunications you don't have the internet and you don't have the ability to do e-commerce and e-business.

I would start with those two sectors.

Ms. RICHARDSON. On a scale of 1 to 5, 5 being best prepared, how would you rate that we would be from an energy perspective?

Ms. HATHAWAY. On a scale of 1 to 5, I think that the energy sector probably was in a better prepared state and it is now going down the scale, as it moves more and more of its infrastructure to an internet-based protocol and as we, the Government, have been offering to the private sector that they need to move more and more of their infrastructure to a smart grid. I don't believe that a smart grid has been approached with the security in mind first and foremost and so, therefore, is making that infrastructure more vulnerable.

Ms. RICHARDSON. Thank you.

Mr. Clinton, according to the White House proposal, companies would be subject to reporting—and it was a previous question by my colleague—would be subject to reporting significant incidents to DHS. Do you have an objection to that?

Mr. CLINTON. Well, the problem is, what is a significant incident? As I tried to articulate in my testimony, there is currently an opinion, a common thought in the press, anyway, that when you have been breached, that is a significant incident. We would probably disagree with that. In the modern world, with modern attacks, virtually everybody gets breached. If you are going to have some of

these advanced persistent threat guys come after you, you are going to be breached, meaning they are going to get in your system.

That means that we have to alter the way we do defense away from perimeter defense, keeping them out, to recognizing them when they are in the system and mitigating the attack there. So even though you may have been breached, that does not mean that it is necessarily a significant incident, because, as I say, these guys are going to get in.

If we made that the line, that you had to report the fact that somebody successfully got into your system and then you were subject to some of these "name and shame" penalties that we discussed earlier, I think that that would be a mistake.

So it really has to do with the definition of what is a significant incident, is where I have my problem.

Ms. RICHARDSON. Ms. Hathaway, would you view a significant incident being a breach, as Mr. Clinton described?

Ms. HATHAWAY. I think a significant incident is any time that you lose confidential information and/or put an operation at risk that it can no longer deliver essential services.

Ms. RICHARDSON. Have you worked with various private industry to define what a significant incident would be?

Ms. HATHAWAY. No, I have not.

Ms. RICHARDSON. Do you have an interest in doing so?

Ms. HATHAWAY. I think that it is important for each sector, whether it is the financial services, defense industrial base, electric power, and the other 17 critical infrastructures, to define what is a significant incident in each one of those sectors and then define the appropriate response and mitigation strategies.

Ms. RICHARDSON. Okay.

Last question, for Mr. Williams: What amount of risk should the Government be responsible for in the event of a major cybersecurity attack in the private sector, if at all?

Mr. WILLIAMS. I think the Government is certainly responsible for collaborating with the private sector if there is an incident. I wouldn't say that that is the same as accepting financial responsibility or operational responsibility. I absolutely believe that as much as possible of both of those need to live with those who have direct ownership of systems and connections.

I would say that in an incident, as in a steady state, if there is a way that we can set up the kind of voluntarily collaboration that I think many of us support, then Government has an obligation to participate in that process. We believe that for DHS; we believe it for our financial regulators. We believe that they have an opportunity to protect other sectors when incidents like that occur. But that is very different from accepting risk and somehow relieving others of that risk.

Ms. RICHARDSON. Thank you.

I yield back.

Mr. LUNGREN. The gentlelady yields back.

The gentleman, Mr. Long, is recognized for 5 minutes.

Mr. LONG. Thank you, Mr. Chairman.

Ms. Hathaway, you spoke about stiffening the penalties. To what degree? Do you agree with the overall proposal, the penalties that

have been proposed in that? What degree do the penalties need to be stiffened to curb some of this activity?

Ms. HATHAWAY. Sir, I think that it is essential that we update the Computer Fraud and Abuse Act. Right now, we do not have enough penalties for the breaches that are happening every day that we read about. I think that the administration's proposal is important.

I would take it one step further and remove the connotation of "protected systems." Protected systems are usually defined as Government and financial institutions. I think that any breach, regardless of where it has happened, in the private sector, the Government, and/or in academia, should be deemed a breach, with the same penalties.

Mr. LONG. Has there been any indication that the penalties that are there now have been effective or the increase that they are going to in years and dollars, do you have any——

Ms. HATHAWAY. I believe that the stiffened and higher penalties, if they are communicated, will start to act as a deterrent, a domestic deterrent. I believe that, also, law enforcement needs to have additional capacity to be able to investigate these breaches and impose those penalties as they find those who are committing those crimes.

Mr. LONG. What percent of cyber attacks would you say are domestic and what percent are non-domestic right now?

Ms. HATHAWAY. I think it would be difficult to quantify the number of incidents and/or breaches. They are going up exponentially every day. I think all countries are suffering the same amount of intrusions.

Mr. LONG. Okay. Thank you.

Mr. Williams, I hail from the Seventh District of Missouri, and we had an incident there where a title company, just a small mom-and-pop shop title company, had, I believe, $440,000 taken out of their account, their bank account, over the weekend. This has been within the last 12 months, maybe a little longer, 15 months, or somewhere in that neighborhood, and had $440,000 wiped out of their account through their bank.

The Secret Service is the investigative arm that looks into that. They have ascertained, I think, that the money first went to Turkey, then Cyprus, ended up in Pakistan. Apparently the hopes of getting it back are about like the hopes of me collecting the $800 million I have been e-mailed here this morning that is in an account in my name.

How can we protect—I mean, this is a mom-and-pop title company. They had the financial resources and backing to be able to go out and qualify for an SBA loan, because, as you know, in a title company, that was not their money they were holding. It was money they were holding for real estate transactions to close. So they at least had the ability to go out and borrow the $440,000, which is not a lot of consolation to them.

But how in the world can we in Congress help the financial services industries in this cyber attack situation?

Mr. WILLIAMS. We certainly can use some help with it. I can tell you some of the things that we are already doing.

One of the evolutions in this whole process over the last few years is that much of the work used to happen solely within an institution, but now it really has to include business clients, like the title company, in the process——

Mr. LONG. And their bank.

Mr. WILLIAMS. And their bank. They absolutely need to be cooperating so that the bank builds secure systems, the title company secures its system and its credentials, so that they have this collaborative arrangement where it is not entirely within the bank's systems and the title company is not entirely on its own in this process.

If we have more research and development, as most of these proposals I think suggest, we will find better and better ways to authenticate, so that if someone over a weekend has gained the credentials of the title company, it will be harder and harder for them to pose as a business client of the bank without the bank being able to detect it.

Mr. LONG. I don't know how we can ever get ahead of the curve on this situation, because it seems like we are constantly behind the curve, and the curve is moving at a rapid pace. So if there anything, off-mike or whatever, later, if you can get to me, as far as how Congress can help, for the entire panel, I would appreciate it.

Mr. WILLIAMS. Yes, sir.

Mr. LONG. Mr. Clinton, you made reference to the fact of insurance two or three times. Walk me through that a little bit. What type of insurance? What do you incentivize? The insurance companies in this, what type of insurance are you talking about?

Mr. CLINTON. Well, there are a variety of insurance instruments that are available—protect against breaches, protect your liability of losses, protect your system, loss of data. It is possible to, for example, in the example of your title company, that they could have bought insurance——

Mr. LONG. You are talking pretty much liability insurance?

Mr. CLINTON. Yes, sir. The typical policies don't tend to cover these cyber events. So there are special instruments that are available for that.

The way that that would probably be best done—there are two things that we propose to get that started, one of which would be for greater information-sharing in return for some sort of Federal benefit. One of the problems the insurance companies have is that they don't have the actuarial data, because companies keep that private. But we believe that, probably, working with the Government, we could get that sort of actuarial data. That will help to bring the rates down. If we can get the rates brought down, then people will sell more insurance, and we can start kind of a virtuous cycle.

The other thing, which is a much bigger idea, would be—we have had this problem of not having enough insurance for an important social good in the past: Crop insurance, flood insurance, et cetera. In those instances, the Federal Government has set up a revolving fund, and that was a better way to manage risk.

This is one of the things I would propose that the committee ought to look at, because right now the Federal Government is carrying all the risk of a major cyber event. If the East Coast goes

down for 3 weeks, Congress is going to pay for it all. That is bad risk management. You ought to be setting up a revolving fund so that we can get some private coverage there.

Mr. LONG. Thank you.

Mr. Chairman, I have no time to yield back, but if I did, trust me, I would.

Mr. LUNGREN. I was going to say, as a conservator, you are not used to giving back something you don't have. But that is all right. I won't interject that.

Mr. Richmond, you are recognized for at least 5 minutes.

Mr. RICHMOND. First of all, Mr. Chairman, let me thank you for having the hearing, and to the Ranking Member who has been very passionate about this issue.

The overwhelming concern that I have—and any of the panelists can chime in—is just the country's awareness of this as a real threat. I chaired Judiciary in the State of Louisiana, which under our jurisdiction we had homeland security and all of those things, and this was not an issue that got a lot of attention, if any.

So what can we do in the importance of raising awareness of it to help combat the threats that we have out there? Just general public awareness, and then we can go from small businesses to major businesses, and then we can just talk about States, because I don't see Louisiana being prepared or being a leader on this at the State level.

So, in any particular order. We could start with you, Ms. Hathaway.

Ms. HATHAWAY. Thank you very much, sir.

I think that we do need to have a National conversation about what is happening on our networks, and it needs to begin really at all levels.

We need to begin the conversation about cybersecurity and network hygiene in the K-through-12 program. As our children are being asked to bring in thumb drives to carry their homework back and forth between school and our home networks, they are being used as a path to actually infect our homes that infect our enterprises which infects our governments and infects our banks. So we need to begin with the children.

If we then move into a university program that extends the Information Assurance Centers of Excellence to all 50 States and beyond 5 percent of our universities, we can start to get to the actual practitioners of and create a stronger workforce.

If we start to have a stronger, more informed workforce on the information security that is trained from K through 12 through university, then we start to have a better-informed workforce and enterprises that can contribute to the National conversation.

I would ask you, as Members, if you could go back and have a conversation in each of one of your districts and start a conversation in the schools and with the enterprises, because I can guarantee you the schools have been breached or the enterprises in your districts have been breached. You can start a simple conversation of what it means to them and what it means to you and how can we begin that National conversation in every district of America.

Mr. SHANNON. Yes. Thank you.

The challenge here is getting people to realize that it is a community impact, that having one organization, one entity, one individual compromised is really not the issue; it is when it happens en masse. So, from CERT's experience, starting with the Morris worm, you know, there was a realization of everyone involved that this is a community event, it is not just their network that has been compromised, not just their host.

So I think part of the challenge, especially when you are looking at insurance issues and regulatory issues, is acknowledging that community aspect. What we find is that organizations, individuals usually are surprised when they realize that the compromise in their system is part of an overall industrialization of the threat and it is affecting the whole community.

So, actually, their—putting themselves at risk, as Ms. Hathaway mentioned, that puts everyone at risk, realizing that we are all in this together. I think that is where the conversation needs to lead. It is not just about your own assets, your own data. Your vulnerabilities actually expose everybody else.

Mr. WILLIAMS. I would have a thought or two at the family or small-business end of the spectrum and at the more corporate end.

At the family level, people shouldn't be worried about advanced persistent threats or some vague notion of identity theft. There are some very concrete things that they can be thinking about. They can be more technology literate from the schools at the children's level and the adults in the home. They can be watching that their PCs and their smart phones have antivirus protection on them, that they are well-maintained. They can be watching their financial statements to ensure that transactions don't appear——

Mr. RICHMOND. Mr. Williams, I know I am going to get cut off in a few minutes. But if you could get me that information or get that to the committee, I think it would be helpful. Because a lot of us send out information to our districts all the time, and that is something that we could put in there, those small things to push people to do.

Before you, Mr. Clinton, I would just—you talked a little bit about "name and shame." Part of the question is the balance between the public's right to know—because a lot of times we, as Government, and private sector, we clash, because the private sector would say, "Nothing bad has happened yet. There is no reason to act until something really, really bad happens." Well, we have to take a different approach, and part of that is to try to make sure nothing ever happens.

So how do we balance "name and shame," as it is described, with the public's right to know and the fact that information is power, and we can prevent it that way, and not just leaving it up the private sector until something bad happens?

I yield back, Mr. Chairman.

Mr. CLINTON. A couple things. I will try to be really quick. Be happy to chat with you more off-line.

First of all, putting in those incentives so that we can get to those best practices and standards that the NSA, CIA, everybody, Secret Service, would solve 90 percent of the problem. That is the first thing we need to do.

With regard to disclosure, ISA is very much in favor of disclosure. But the disclosure, as I have detailed in my testimony, the disclosures have been to be purposeful disclosures. The public's right to be secure, I would say, is the higher value here.

What we have proposed is, instead of having general broad disclosure, which will go to the press, which will treat it sensationally, will skip over the details as to whether or not this was really harm here or not, we would propose more of a CDC sort of model. That is where the reporting ought to be. It should be going into entities that can understand the real problem and can work on solving the problem so that we don't have the losses that come out.

One of the problems here is our definitions. Think of cybersecurity like a football game, okay? If you are the defense in a football game, it is not a—everybody gives up yards, right? So the fact that you have been breached, that is not the problem. The problem is when the offense scores. So you can have breaches that don't lead to scores.

We shouldn't be putting out publications, you know, and having news conferences about somebody being—you know, somebody losing just some yardage. We should confine that to experts detailing when there has actually been losses, and then we can deal with, you know, some sort of SEC filings that are appropriate, which the SEC already will do.

So we are arguing for a more sophisticated form of disclosure to deal with a more sophisticated sort of attack. We think that that will lead to greater security, which is our goal.

Mr. LUNGREN. Now, the gentleman, Mr. Marino, a great football fan, is recognized for 5 minutes to continue the analogy.

Mr. MARINO. Thank you, Mr. Chairman.

Carrying that ball down the field on the offensive end of things, I want to turn this conversation a little bit. We are talking about the breaching of the systems and increasing the penalties. But I find it ironic that we are here—and, obviously, I am a big supporter of public hearings—but we are here talking about security measures, which—we could have a hacker sitting out in the audience.

So where do we draw that line between sharing public information and not sharing it to prevent it from the hackers getting control of it? But, by the same token, the hackers are pretty sharp. No. 2, as far as penalty-wise, what do we do with the 15-year-old genius who gets into the system just for fun and causes havoc?

With those two questions, could we start with Ms. Hathaway? My father told me ladies before gentlemen.

Ms. HATHAWAY. Well, let me start with the 15-year-old genius. There are some efforts within the law enforcement community and with the actual school districts to identify those genius hackers. Instead of a sentencing or going to juvenile hall, they actually start working with the law enforcement community or get prepared to work for our intelligence community. So they are the next-generation workforce with the skill set that we need.

Mr. MARINO. Okay. Let me interrupt just for a moment. Primarily—and the former attorney general from California will agree with me, I think, that the Federal system has very little jurisdiction or, actually, maybe no ability to deal with juveniles.

Ms. HATHAWAY. I understand that the law enforcement community has been working with the high schools to actually help identify and work with using their skill set and turning it to good as opposed to harm.

Mr. MARINO. I understand that. But how about the penalty aspect of it? What is your position on that? Do you have a suggestion on that?

Ms. HATHAWAY. I think that penalties for kids, we need to look into, the penalty could actually be serving, you know, for the U.S. Government or serving on behalf of the communities to actually go out and prosecute.

Mr. MARINO. Mr. Shannon.

Mr. SHANNON. Could you repeat the question? I have lost the track of what you—the first part of the question.

Mr. MARINO. The two questions were: Keeping it confidential; and how do we deal with the juveniles? Because the Federal system is not that well-equipped to deal with juveniles when it comes to penalties.

Mr. SHANNON. Yeah, I will deal with the confidentiality issue.

One of the great innovations of the internet is the freedom to express yourself, the freedom to create new technical capabilities, to innovate quickly. It is enabled by open disclosure, open sharing of information.

Clearly, disclosing vulnerabilities is a challenge, but when you realize that there is a threat and there is a remediation, sharing that quickly and openly is better than what is the alternative, remaining ignorant. Because I can assure you that the hackers do know, and if you try and communicate it in some out of sort of closed or secure manner, once you get to sufficient scale, they will still know. So, you know, there is no hiding it, in that sense.

So it is better to put the information out there, let people be informed, and then they can make the appropriate decision, especially when it comes to a mitigation.

Mr. MARINO. Okay.

Mr. Williams.

Mr. WILLIAMS. I think, quite appropriately, most of this conversation already occurs in confidential spheres and should continue that way. So companies, when they contract with other companies, will talk very explicitly about their security posture. That has a very strong market incentive for people to do the right thing.

In our industry, institutions talk with their regulators, but they do that almost exclusively behind closed doors. The kind of sharing that I think the administration proposal contemplates would also be confidential, two-way sharing between DHS and some of the other agencies and the companies.

There are, I think, a couple of exceptions to this idea that there should be a cloak of confidentiality generally. One is, if there is information that can help consumers to protect themselves, if an individual consumer has been put at risk, there are and should be rules to ensure that that person knows what they need to know to protect themselves. The same at the SEC level for investors.

Mr. MARINO. Okay. All right. Thank you.

Mr. Clinton, you have 18 seconds.

Mr. CLINTON. We are dealing with different levels of data, so the sophisticates ought to be meeting amongst themselves and sharing data and then atomizing it and then have it pushed out to the broader community.

We have a proposal we actually started with Melissa Hathaway a couple of years ago with DHS to do exactly that. I would be happy to talk with you more off-line.

Mr. MARINO. Thank you. Touchdown.

Thank you very much, Mr. Chairman.

Mr. LUNGREN. Now I will be happy to recognize the gentleman in this Congress who probably was happier than any other Member that Whitey Bulger got nabbed yesterday, Mr. Keating.

Mr. KEATING. Happy and relieved.

You know, interestingly enough—I will just a little share information with you—in terms of getting the word out, I was struck by the fact that there is a group in the Boston area where the 30 top executives, largest firms, they meet usually annually to discuss what their biggest issue is. That could be taxes, it could be anything; it is open-ended. They decided it was cybersecurity. So I do think that people understand the magnitude and the importance of this, and that is out there.

What I am struggling with is this, and I don't know if there is an answer. Mr. Clinton started down that track, but I would just like to ask the rest of the panel if they could help in this regard. I am looking for something, an existing model, public-private model, quasi-governmental model, that already is there, may not be a perfect fit, but just to give me an idea of where the Chairman said, the sweet spot is. We are looking for something that is flexible enough so that regulations don't smother the ability and provide deterrence.

But I don't agree with, you know, the CDC model approach, that, you know, it is just out there. I think we have to more oversight proactively on that. I don't know where that is. I know that the "name and shame" issue can, I think, be mitigated by having, you know, rankings, the way they do in financial institutions. When they do an audit, you can have CAMEL ratings, whatever ratings they might be—1, 2, 3, 4—and you are in categories where, you know, companies will have some responsibility, and insurance companies can look at that as well.

But if you could—and I don't anticipate anyone has a perfect fit—can you think of some existing models in other areas? You know, Mr. Clinton has mentioned the CDC. I would like to ask the other panelists.

Mr. SHANNON. So I think there are a couple of models. There is the automotive and airline industry that, you know, have reporting on accidents and incidents that allows for an appropriate oversight. So it is a more closed—the NTSB, you know, has a closed investigation when an incident happens.

I think it is important also to look at the CDC model and think about where it actually is appropriate and where it is not appropriate. I mean, where it is not appropriate maybe is nation-state threats. But certainly in terms of deal with industrial challenges in malware and exploitation, being able to have a better situational

awareness based on the preponderance of incidents is what is needed.

An individual, just because I got hacked, I don't know if I am the only one in the world or whatever. But if the Government wants to or organizations want to be able to do a broad response, having that sort of situational awareness is imperative. Otherwise, you don't know that there is a challenge.

Mr. KEATING. Thank you, Dr. Shannon. That is great after something has happened, too, and that is important.

What about trying to prevent areas and to rank or to find some kind of oversight that is not too, you know, over-regulatory in nature?

Mr. SHANNON. I will defer to my colleagues. We deal with things when——

Mr. KEATING. That is all right. Thank you.

Mr. WILLIAMS. If I might, one macro example, one micro example.

A macro example I think is environmental protection. There was a time when the best thinking on environmental protection was simple command-and-control regulation. I don't think that is the right model for us here.

But over time, environmental protection advocates realized that industry needed to be at the table in determining what the solution was and then also needed to be at the table in executing it. I think that is where we are in cybersecurity. We need to work together to figure out what the right answers are and then to deliver them.

The micro example, just the information-sharing and analysis center within our sector I think is a good model of public-private collaboration. It is largely chartered and, in many ways, supported by Government resources. It helps us connect with other sectors. But it is a private-led, voluntary effort that we think has brought us great progress.

Mr. KEATING. Ms. Hathaway, did you have any thoughts?

Ms. HATHAWAY. I think that there is a lot that could be done by turning to the internet service providers and the telecommunications companies as the first order of warning and defense.

Australia has adopted a code of practice or a code of conduct where 90 percent of their telecommunications providers have opted in, without regulation, to provide that service to the core infrastructure. Europe, within the European Union, have adopted Telecommunications Directive 13a, which is regulating all of the internet service providers within all 27 countries to provide that service across their infrastructure.

I think that the United States could learn from those different experiments and/or capabilities and understand what the costs are to better clean and keep our infrastructure clean and warn us of the impending threats.

Mr. KEATING. Great. Thank you very much.

Mr. LUNGREN. I thank my fellow Members of the subcommittee for attending.

I thank the witnesses for their valuable testimony. This has been very, very helpful. It is the beginning of the inquiry, in a real sense, rather than the end of it.

Members of the committee may have some additional questions for the witnesses, and we would ask you to please respond to those in writing. The hearing record will be held open for 10 days.

The subcommittee stands adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR MELISSA HATHAWAY

Question 1. From media reports, China is engaged in the most damaging hacking campaign in history. At the same time, its primary telecommunications equipment provider continues to gain U.S. market share, including in the Federal market.

What solutions can the Federal Government pursue against foreign espionage? How can the private sector protect against the threat?

Answer. The Webster's definition of espionage is, "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."[1] There is a long history of espionage and in general, it is a globally accepted practice of intelligence collection to better understand Government and company intentions. The National Counter Intelligence Executive (NCIX) tracks these trends and reports to Congress the status of foreign economic collection efforts and industrial espionage.[2] In its fiscal year 2008 annual report, NCIX reported that "foreign economic intelligence collection and industrial espionage has continued unabated."[3] The newspapers highlight everyday that companies and governments regularly face attempts by others to gain unauthorized access through the internet to the information technology systems by, for example, masquerading as authorized users or through the surreptitious introduction of software. However, this does not negate the need to limit foreign espionage that has become increasingly more pervasive and sophisticated against our public and private sectors. Furthermore, focusing on one opponent may distract our industry and Government from implementing a more complete strategy.

Potential Solutions

- The Federal Bureau of Investigation (FBI) and the intelligence community need to better inform industry of the threats they are facing and how they are being exploited or penetrated. A training program to educate 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, would go a long way to reducing the number of incidents and loss of confidential information.
- DoD is proposing to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clauses to address requirements for safeguarding unclassified DoD information. This development is essential because emerging, pre-classified military technologies or commercial breakthrough technologies are increasingly becoming the target of espionage. The proposed DFAR changes would require industry to implement basic security measures to increase their defenses from cyber intruders.
- Engage the United States Department of State's International Telecommunication Advisory Committee (ITAC)[4] and the Advisory Committee on Inter-

---

[1] *http://www.merriam-webster.com/dictionary/espionage.*

[2] Industrial espionage, which is the knowing misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret. Misappropriation includes, but is not limited to stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to misappropriate trade secrets without authorization. Industrial espionage is also criminalized under the Economic Espionage Act.

[3] *http://www.ncix.gov/publications/reports/fecie_all/fecie_2008/2008_FECIE_Blue.pdf.*

[4] The United States International Telecommunication Advisory Committee (ITAC) advises the Department of State in the preparation of U.S. positions for meetings of international treaty organizations, develops and coordinates proposed contributions to international meetings as U.S. contributions, and advises the Department on other matters to be undertaken by the United States at these international meetings. The international meetings addressed by the ITAC are

Continued

national Communications and Information Policy (ACICIP)[5] to better understand predatory trade practices in the United States and elsewhere and develop strategies to respond to these practices in a timely manner. Use these advisory councils and others to gain a better understanding of what trade and economic implications are to U.S.-based corporations if other countries impose a Committee for Foreign Investment in the United States (CFIUS) like regime to protect their respective National and economic security interests.

- Congress should consider updating the Economic Espionage[6] Act of 1996. While the definition of trade secret is consistent with the Uniform Trade Secrets Act, which states that the information is subject to reasonable measures to preserve its secrecy and derives independent economic value from not being generally known to or ascertainable by the public, the threshold for protection is too high. As such, industry is required at the onset of the development to protect any idea as a trade secret. Addressing the broad-based economic industrial espionage that we are observing on our corporate networks requires that the Government lower the threshold for a trade secret or add a threshold around proprietary information.

Question 2. A large issue facing appropriate risk management for Government and critical infrastructure is supply chain risk management since so much of our software and IT equipment is manufactured overseas.

What's the best approach for better evaluating the security of our IT supply chain?

Answer. The internet and the information communications infrastructure has evolved and has been enhanced by global commercial innovation. While the United States incubated its beginning through the Advanced Research Projects Agency (ARPA) in the late 1960s, and helped it flourish through Palo Alto Research Center and the companies of silicon valley, its evolution and the attendant benefits to society have come from many other countries and global corporations. Our infrastructure is dependent on this global marketplace and our economy is dependent upon this backbone remaining secure and resilient. A broad, holistic approach to risk management is required rather than a wholesale condemnation of off-shore development, foreign products and services, or foreign ownership.

The best approach to securing our IT supply chain is one that is transparent, mindful of unintended second order consequences, and aids in decision making. We must recognize that the supply chain consists of many phases: Design, manufacture, integrate, distribute, install and operate, maintain, and retire—and any conversation regarding security of the supply chain must apply to the entire lifecycle. To meet tomorrow's threats, we must develop protection measures across the product lifecycle and reinforce these measures through acquisition processes and effective implementation of agency security practices. For example, the highest risks in the supply chain are "after build" (e.g. install and operate and retire phases) because this is where multiple vendors participate in the process (e.g., integrate products with other systems, patch/update, etc.) and there are few measures to monitor and assure integrity throughout the entire process.

To understand alternative approaches will require a partnership with industry that assures coordination and buy-in that enables industry to "do the right thing" and not be penalized in the process. A dialogue has begun via the Open Group Trusted Technology Forum and it enjoys international participation by governments and industry alike. The Open Trusted Technology Provider Framework sets forth best practices identified by a cross-industry forum which, if used by a technology vendor, may allow a Government or commercial enterprise customer to consider the vendor's products as more secure and trusted.

---

those of the International Telecommunication Union, the Inter-American Telecommunication Commission (CITEL) of the Organization of American States, the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC). Members of the ITAC are drawn from the Government, network operators, service providers, and manufacturers involved in the telecommunications sector.

[5] The Advisory Committee on International Communications and Information Policy (ACICIP) serves the Department of State in an advisory capacity concerning major economic, social, and legal issues and problems in international communications and information policy. These issues and problems involve users and providers of information and communication services, technology research and development, foreign industrial and regulatory policy, the activities of international organizations in communications and information, and developing country interests.

[6] Economic espionage, which is the knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization. Section 101(a) of the Economic Espionage Act (EEA) of 1996 criminalizes economic espionage.

Moreover, the Cyberspace Policy Review called for the need to "define procurement strategies through the General Services Administration, building on work by the National Security Agency for the Department of Defense, for commercial products and services in order to create market incentives for security to be part of hardware and software product designs, new security technologies, and secure managed services." The efforts of the United States General Services Administration (GSA) in working to address this requirement through the SmartBUY blanket purchase agreement awards aimed at providing better cybersecurity protection to Federal, State, local, and Tribal governments should be strongly supported. Under its new Federal-wide Situational Awareness and Incident Response (SAIR) Tier II cybersecurity initiative, GSA will use the procurement process to help protect our IT infrastructure from cybersecurity incidents and other vulnerabilities, while providing maximum value for taxpayer dollars.

These two initiatives are good steps toward enhancing the security of the supply chain while at the same time being mindful of market forces.

Question 3. Will the administration's proposal of DHS authority over the private sector—which envisions Federal "framework," used to develop cyber plans, and a subsequent evaluation of those plans—provide the necessary flexibility to optimize private sector security?

Answer. Not necessarily. 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."[7] 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 risk. Inserting DHS into a regulator role runs the risk of diluting its operational and policy responsibilities, which would 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.[8] 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 to the SEC, which is the Executive Branch Independent Agency responsible for this type of reporting, and not add an additional mission responsibility to DHS.

Question 4. Will the authorizations for DHS to "work with" the Federal Acquisitions Regulatory (FAR) Council to improve supply chain security have any practical effect?

Answer. It is unclear. Adjusting the way that the Government procures goods and services can be a catalyst for change but may not necessarily make a material difference in the security of the supply chain. The key is to decide what are the measures of performance that are desired and under what conditions? If the level of security assurance increases, but price goes up unacceptably, is that success? Changes to the FAR can certainly result in change to business processes. The changes in business processes may result in increased costs which will be passed onto the Government and other customers.

It also is important to realize that any change to the FAR may not apply across the Federal Government. Some agencies are exempt from these rules including: the Central Intelligence Agency, the United States Postal Service, the Tennessee Valley Authority, the Federal Aviation Administration, and the Bonneville Power Administration. In these cases, the agency promulgates its own specific procurement rules.

Question 5a. The White House has directed that all Federal Departments and Agencies move a portion of their data processing and storage to the cloud in the coming years.

While that strategy is a good one when it comes to making the most of Federal IT spending in these fiscally demanding times, how can the security of the cloud be evaluate and improved to ensure that we're not taking unnecessary risks with mission-critical data?

Answer. According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources [e.g., networks, servers, storage, applications, and services] that can be rapidly provisioned and released with minimal management effort or service provider interaction." The key tenet of the cloud is availability. But the other two cornerstones of information security—integrity and

[7] The White House. Cybersecurity Legislative Package: Cybersecurity Regulatory Framework For Covered Critical Infrastructure Act.

[8] Senator Rockefeller letter to SEC Chairman Mary Schapiro. 11 May 2011.

availability—are not readily commanded by the cloud environment. The October 2010 report from Forrester on cloud security states that security is the single biggest barrier to broad cloud adoption.

In December 2010, the Office of Management and Budget (OMB) issued a report entitled the "25 Point Plan to Reform Federal Information Technology Management" and in February 2011 it published another report entitled, the "Federal Cloud Computing Strategy," where it articulated the need for: Consolidation, efficiency, and reduction in IT spend. The second report directed each department and agency to identify three "must move" services within 3 months, and move one of those services to the cloud within 12 months and the remaining two within 18 months. Most departments and agencies are looking to move email to the cloud as their first project.

The GSA is developing a contract vehicle to service agency needs for cloud computing, entitled Federal Risk and Authorization Management Program (FedRAMP). Many within industry are raising substantive concerns with the proposed controls and specifications as being too difficult and costly, and that they potentially could prevent vendors from being able to move agency computing operations to the cloud by the deadline. Any cloud environment that is to be used to process Government workloads must be able, at a minimum, to demonstrate that it provides the same level of security (as defined in the question) as a traditional system. Currently, this is demonstrated via a Federal Information Security Management Act (FISMA) certification and accreditation (C&A) process, which process has been roundly criticized as a compliance-based framework focused upon a snap-shot in time. While one can argue that a cloud computing environment can be made more secure than a traditional one by leveraging certain aspects and features of virtualization and other enabling cloud technologies, the security ecosystem (technologies, control frameworks, audit procedures, threat models, etc.) must account for the unique attributes and vulnerabilities of cloud computing to be relevant.

Having said that, several large-scale efforts are in progress, in both Government and industry, to rigorously measure risk related to cloud computing implementation. Among these are: (1) The "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing", drafted and released for comment and public input jointly by National Institute for Standards and Technologies (NIST), GSA, the Federal CIO Council, and some of its subordinate working bodies; (2) the Cloud Security Alliance, an industry association centered on cloud computing, has developed a Cloud Controls Matrix, which cross-connects established security requirements in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, International Standards Organization (ISO), IEEE, NIST publications, FedRAMP, and other sources; and (3) the Defense Science Board has launched a task force to review cybersecurity and reliability in a digital cloud. There is broad agreement among serious information security practitioners that the task of defining security standards for cloud computing is a work in progress, and several organizations have commissioned studies, (e.g., the Intelligence and National Security Alliance (INSA) and the Armed Forces Communications and Electronics Association (AFCEA)) now in progress, to evaluate and report on specific aspects of the subject. In my opinion, one of the best, objective reports that describes the opportunities and vulnerabilities associated with cloud computing, is one that was published in November of 2010 by the European Network and Information Security Agency (ENISA), entitled: *Cloud Computing: Benefits, Risks, and Recommendations for Information Security.*

Question 5b. How can continuous monitoring be implemented in the cloud environment? Do you have any current examples of strong security in the cloud?

Answer. It is important to recognize that the term "cloud computing" embraces several different technical and process models, which by their nature have highly-differentiated levels of monitoring and control by sponsoring organizations/hosts, and concomitantly, very-different levels of active participation by hosted entities. And when considering these, one must keep in mind that the implementation of the cloud is the most important aspect and no two clouds are implemented exactly the same.

How continuous monitoring gets implemented in the cloud very much depends on the type of cloud environment and the willingness and capabilities of the provider to conduct continuous monitoring activities. There are numerous technologies that exist today or that are in development to enable the monitoring of the cloud (e.g., infrastructure, systems, and data). The real question is: What is being monitored and does it actually correspond to the proper threat model? The United States Department of State may be an example to turn to as it has the "first mover advantage" for use of a secure cloud environment. It is applying a high degree of rigor in timely scanning and prioritized remediation through continuous monitoring—thereby providing a more secure common baseline for all.

As such, there can be no general answer to this question. However, certain "private clouds", hosted by highly-competent security organizations and providing infrastructure, platform, and/or software services to members of their own organization only, may be considered highly-secure. Examples would include certain clouds developed and used inside National intelligence agencies, hosted on-site and with access limited to authorized employees of those organizations. In such cases, the economic virtues of efficiency and economy of scale is use of IT resources may accrue, but security of hosted data, participants, infrastructure, and services are all tightly controlled.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR GREGORY E. SHANNON

Question 1a. DHS has been developing the National Cyber Incident Response Plan, which it exercises through its bi-annual response plan.

What more should the Federal Government be doing to improve response to cyber attacks?

Answer. Encourage more frequent agency and interagency cyber exercises that will identify technological and procedural gaps as well as build working relationships and trust both within and across agencies. For any response activity to be effective the organizations that participate in the response need regular, structured, measured practice, weekly or monthly if possible. This practice builds common understanding of the processes and technologies to be used as well as builds trust among the various participants. These exercises need not be immense/expensive; smaller-scale exercises testing various subcomponents of a response plan on a regular basis would be valuable and cost-effective.

Support timely access to operational situation and incident data. The Federal Government should study the history of the PCII program and the lessons learned to update it to be more attractive to industry.

Encourage making meaningful sets of operational data accessible to researchers so that they can determine what data is best to share and what prevention/response tactics are most effective.

Question 1b. Are there priorities for DHS response planning that would be helpful to include in legislation?

Answer. Priority: How the Federal Government should engage the private sector in a major incident—what information should agencies provide and when will they provide it? Plans should include: How to engage the private sector in a major incident, which entities does the Government need cooperation from, and how is best to collaborate? This will make the Government more predictable; allowing the private sector to then plan appropriately.

Priority: Grant Federal CIOs more authority for protecting their cyber infrastructures before incidents occur. It's difficult, if not impossible, to defend that for which one had no hand in creating.

Question 2. When CMU–CERT is engaged in a response to a cyber attack, what is the greatest difficulty of getting information from the private sector?

Answer. There are several significant barriers to getting the private sector to share information.

The Federal Government is frequently hard-pressed to convince the private sector that there is real value in sharing information with them. The perception continues to be that when industry shares information they receive nothing (or nothing of value) in return from the Government. CERT has been a part of successful models, such as the work done by DC3 in the operation of the DoD-Defense Industrial Base Collaborative Information Sharing Environment (D–CISE), whose example could be built upon in other critical infrastructure sectors. It takes effort to demonstrate to the private sector that the Government can be helpful; e.g. by extracting indicators from sensitive data or by creating the environments and the tools for cleansing data so it cannot be attributed to its source and thereby shared with the private sector. Additionally, the private sector has multiple concerns about the potential adverse effects of sharing information—those barriers, such as fines, litigation, etc. should be identified and eliminated through incentives and safe harbors, where possible.

On the other hand, while some entities might not want to share, a large number of companies (particular small- to medium-sized businesses) do not have the capabilities to collect and/or analyze the data that is necessary for their own protection much less useful to the Government. What needs to be shared is actionable information and the capability to successfully implement the actions must still be built. The Government could encourage industry to develop the competency using incentives (e.g. the Government could consider subsidizing these competencies thru CNDSP or MSSP models).

How information comes to the Government can also have significant impact on whether or not the Government can disseminate critical data to prevent further impact to other entities. In many cases, the Government knows what is happening, but effective communication of remediation information is often limited. At times, information comes in via reporting with so many restrictions that the Federal Government cannot share the data. Savvy organizations are realizing that they can "have their cake and eat it too" by complying with the reporting requirements but while still ensuring that no data, remediation information, or conclusions from their incident is distributed.

Lastly, the Government, in its handling of classified information, should examine current practices to find effective ways to separate actionable information from classified or privileged data so that incident data can be used to help others protect themselves.

Question 3a. How do we bridge the gap between operations and research to transition technology in a timely and effective manner?

Answer. In order to effectively transition research for real-time operations there must be stronger feedback mechanisms between operations and research.

We believe CERT is a successful model that brings together researchers and operators and could be an effective paradigm for others. The CERT Program at the SEI, through its customer engagements with security operations centers, network operators, vulnerability and malicious code analysis centers, incident response teams, law enforcement investigators, and intelligence analysts, has a first-hand view into the state of security in our National critical information infrastructures. This view helps us understand the security strengths and weaknesses of fielded technology and systems, the evolving threats and associated attack methods and tools, the effectiveness of current security technologies and practices, and the security needs of system operators. Empirical data from our DoD and other Government customer engagements ensure our research and development agenda is grounded in operational problems and realities, and we are addressing significant problems for which effective solutions do not currently exist. This model also creates an environment where solutions can be rapidly deployed and prototyping with strategic customers helps set realistic transition paths for the broader community.

The challenge in transitioning potentially important cybersecurity innovations from small companies and startups is especially profound. Having spent half of my (Dr. Shannon) career in such companies, I know this challenge first-hand; it is difficult, if not impossible, to get timely operational feedback on one's technology when dealing with Government customers. I encourage the subcommittee to support efforts to bring together operationally relevant data and small companies so that: (1) Government entities can determine if there's promise in the technology, and (2) the small company can quickly iterate and adapt to the realities of the operational data.

The challenge is to create a continuous capability with steady inflows of technologies, operational knowledge, and Government needs. CERT/SEI/CMU is already doing this successfully but intermittently for specific customers with innovations from academia. Sustaining this activity at CERT and elsewhere and expanding it to small companies would improve the flow of effective cybersecurity and incident response innovations into the Government.

Question 3b. And what resources are needed?

Answer. The Government would greatly benefit from establishing and maintaining a sustained cybersecurity and response innovation acceleration program focused on transitioning innovations from the private sector to the Government with subsidies for small businesses and universities and incentives for larger businesses. This endeavor could be funded at $4–6 million/year and would bring four essential elements together: Unique operational data sources, private innovations, informed scientific evaluation, and Government needs. The goal, from first contact with a company, would be to operationally deploy their validated innovation(s) in less than a year within some meaningful part of the Government.

Question 4. How can we increase our confidence in the various technical and policy solutions proposed at any point will be as effective as promised/implied?

Answer. Encourage the use of scientifically validated metrics and measurements in studies about proposed solutions. Too often cybersecurity solutions proposed have been based on limited evidence and/or scientifically unvalidated data and techniques.

The ability to measure effectiveness of technology and new policy is an area sorely in need of research and deeply in need of funding. I (Dr. Shannon) am truly humbled at how little that we experts say we "know" about cybersecurity and incident response that has actually been scientifically validated. Research sponsors should be encouraged to invest in "the empirical science of cybersecurity", including the devel-

opment of metrics and experimental methods that support measurement of the effectiveness and cost/benefit of proposed security solutions.

Question 5a. In your testimony you mention that the Government should focus on three things to improve incident response capability, information sharing, forensic analysis capability and training.

Focusing on information sharing, in your opinion does requiring reporting improve the quality of reporting or just the quantity?

Answer. Today, such a requirement would only increase the quantity. Per our answers to the other questions above, research into what is the right data to share as well as cost-effective means to collect and analyze the data will enable mandatory reporting requirements to improve the quality of the data.

With mandatory reporting requirements should come clear guidance on what data and associated meta-data needs to be shared; under what circumstances; ideally normalized using a common taxonomy represented and exchanged using standardized formats and protocols. Research is needed in these areas; NIST and others are already working on some of these issues. How the data should look (form/format) is the easy part; what data is most useful is much harder.

Question 5b. Can too much information actually be a problem or can there never be too little information when it comes to cybersecurity incidents?

Answer. Since a cybersecurity incident investigation often starts as an attempt to discover the true scope and scale of what transpired, various data sources need to be synthesized. The issue is not necessarily having more data, but the right data. We frequently see cases where information collected and shared is useless. Without context about the incident, it is difficult to abstractly predict what might be needed in advance. There is inherent cost in extracting and delivering the data. Hence, it is convenient to know what data is available and to be able to request it on demand. Achieving this enhanced situational awareness will require continued research and pilot programs with data owners.

Question 6. How can legislation assist in facilitating capable, scalable, and cost-effective cyber incident response for Government and critical infrastructure?

Answer.

- Encourage public/private cooperation and access to data for empirical research.
- Support training operators in the same context as they work.
- Support scalable forensics capabilities.
- Regularly recognize successes in cybersecurity and incident response.

Successful response requires close cooperation between the Government and the private sector, so as mentioned in question No. 1, inclusion of the private sector in plans for incident response would greatly improve response effectiveness. Expanding the scope of the current policies to include plans for working with industry would allow for more timely and capable responses. Cooperation should also include access for innovators to incident data, which will result in better, scientifically validated solutions. Additionally, the Government must continue to engage the community at large to maintain perspective on what currently exists, both in terms of technological gaps and solutions.

People who respond to cyber incidents must be adequately trained. The Government needs a training solution that is scalable and cost-effective, such as CERT's Virtual Training Environment (VTE) and X–NET.

Traditional training and education models still employ brick and mortar classrooms to provide infrequent instruction directed at individual students. These models simply cannot keep up with the pace of change or provide successful and cost-effective mechanisms for organizations to gain and maintain the real-world experience needed to operate effectively in cyberspace. Civilian employees cannot use production agency networks for operational training and ranges or laboratory environments can be costly to develop, operate, and maintain.

In addition to training and practice limitations, agencies currently do not have any reliable capability to assess the operational mission readiness of their cyber workforce. The current unit-level cyber assessment mechanisms rely on artificial paper-based simulations and "cyber-add-ons" to intra- and interagency exercises. Neither approach provides for reliable mission-readiness evaluation and reporting of workforce effectiveness.

CERT's VTE provides rich media instruction and hands-on training labs to remote students over the internet. It enables students to access high-quality training on security, computer forensics, and incident response anywhere in the world, with only a web browser and an internet connection. What's more, VTE is a cost-effective way

to train the workforce,[1] and has no expiration date, allowing students access to all training modules as often as they want and for as long as they want after completing training. Students can continually return to the module to practice and test the network, closing the gap between learning a concept and using that concept.

CERT's Exercise Network (XNET) provides real-world experience building and readiness evaluation via synchronous, team-based, scenario-driven cyber exercises. Experience through routine practice is known to be the decisive factor in how effectively individuals and organizations respond during incidents and emergency situations. XNET is designed to make this routine practice web-accessible for globally distributed teams and units.

The Federal Government needs to address its current backlog of cyber forensics data, as well as, collect forensics data in on-going cases in a timely and cost-effective manner. To help augment the cyber forensic capabilities of law enforcement the CERT program created the Clustered-Computing Analysis Platform (C–CAP). C–CAP is designed to support 200 concurrent computer examinations looking at 200 terabytes of data, allowing for a massive, coordinated effort. Absent catastrophic events, the C–CAP environment can offer underequipped or overwhelmed agencies real-time additional resources. C–CAP is a state-of-the-art forensics analysis environment that provides a complete suite of tools for host-based and network investigations. C–CAP augments scarce resources by allowing multiple users to view the same data, either remotely or locally; while maximizing the application of specialized computing resources to the forensic and incident response missions. Analysts and investigators enjoy flexible, secure access to high-performance systems, increasing productivity and facilitating distributed collaboration. Designed specifically for forensics and incident response analysis, this unique integration and packaging of tools, accelerates the analysis processes, maximizes performance and reduces costs. C–CAP is a flexible solution, allowing agencies to add or remove components that are relevant to their particular needs. Its unique centralized management interface allows organizations to rapidly allocate platform resources to tasks or analysts. Scalable and cost-effective, C–CAP can be customized to suit any organization, regardless of size and mission.

Finally, we recommend that the Government recognize and reward good examples of secure systems and practices. In the end, infrastructure components need to be built more securely in the first place and by highlighting those organizations who are doing it right, the Government can incentive others. The Baldrige Program is administered by the National Institute of Standards (NIST) and educates organizations in performance excellence management and administers the Malcolm Baldrige National Quality Award. This public-private partnership is helping organizations achieve best-in-class levels of performance; identifying and recognizing role-model organizations; identifying and sharing best management practices, principles, and strategies. A similar program or award in the area of security and resiliency could yield substantial benefits.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR LEIGH WILLIAMS

Question 1a. You describe a large number of items members of the financial services sector undertake with respect to cybersecurity.

Can you compare these activities with those of the other sectors?

Answer. We are not in a position to compare the quality or quantity of cybersecurity efforts in other sectors to financial services, but we can identify some similarities and differences. As a similarity, we recognize that individual companies in telecommunications and information technology invest heavily in cybersecurity and resiliency. We understand that one difference is that financial institutions may do more collaborative work because they are so technically and commercially interconnected and because regulations tend to promote standardization.

Question 1b. Which of these activities are the product of voluntary action by the BITS community and which are the result of Federal or State regulations?

---

[1] High-Fidelity e-Learning: SEI's Virtual Training Environment (VTE): TECHNICAL REPORT CMU/SEI–2009–TR–005 ESC–TR–2009–005: VTE was used to deliver 38,157 hours of training for DISA during the period from January 1, 2007 through October 31, 2007. The American Society of Training and Development (ASTD) reports that the average cost per learning hour delivered by its members in 2006 was $54.25. According to the ASTD data, the value of VTE-delivered training is therefore $2,070,017 ($54.25 per hour × 38,157 hours = $2,070,017.25). The total cost to DISA for the VTE-delivered training was $858,250. This represents a cost savings to the DISA of $1,211,767 as compared to what they could have expected to pay at prevailing industry average costs. The total return on investment for the DISA is 141 percent. (($2,070,017 – $858,250) / $858,250 = 141%).

Answer. At the institution level, most BITS members' cybersecurity programs are primarily motivated by business and customer interests. Regulations sometimes reinforce these motivations, but also sometimes require slightly different solutions. For example, under Gramm-Leach-Bliley, banks are required to have security programs that incorporate specific elements and that are reviewed by their boards. Without the regulation, the vast majority of banks would still have plans, but perhaps with different mixes of elements, and with review processes specific to their governance strategies. At the industry level—in efforts such as the mobile, cloud, social networking, and malware efforts mentioned in our June 24 testimony—virtually all of the collaboration is purely voluntary.

Question 1c. What is the cost of complying with these activities?

Answer. We do not have a specific estimate of regulatory compliance costs in cybersecurity. We do believe, however, that elevated compliance costs can crowd out risk management spending and investments in innovation, and can increase costs to customers and reduce institutions' returns.

Question 2. Under the administration's proposal what new cybersecurity activities would BITS members undertake that they are not now doing?

Answer. Under the administration proposal, there would be at least two ways in which BITS members could more effectively share information with other sectors. First, because other sectors could be prompted to produce more information and DHS would be tasked with aggregating it, there would be more information available to exchange with our colleagues in other sectors. Second, the safe harbor and confidentiality provisions would reduce the risk of actively sharing information with the other critical infrastructures and with DHS.

Question 3. You are endorsing the administration's legislative proposal, which does not carve out the financial sector from its reach.

With this endorsement is it to safe to assume that the financial industry will not be lobbying for a carve-out or any special treatment if the administration's proposal moves forward?

Answer. BITS does not intend to advocate for the financial services sector to be carved out. BITS and its members do believe that the existing financial regulatory frameworks and the proposed approach will have to be reconciled. As we testified, this could be accomplished, for example, by recognizing where substantially similar requirements already exist, by leaving substantial authority within the sector, by requiring DHS to work through the sector-specific agencies and primary regulators, or by DHS delegating authority back to the sector-specific agencies and primary regulators.

Question 4a. Your testimony praises the administration's legislative proposal for a variety of things like coordinating with companies and other agencies; however, it was my understanding that most, if not all, these activities are currently going on without this legislation.

Which specific provisions of the administration's proposal will cause BITS members to make security improvements beyond their current activities and why is legislation required to get the BITS membership to undertake these activities?

Answer. Yes, BITS members are already satisfying many of the requirements of the administration's proposal. The value of the proposal does not arise primarily from BITS members individually improving their security programs. Much of the value arises from companies in multiple industries and Federal agencies with various missions working in closer cooperation on common problems. We think this is happening reasonably well within our sector, but we see room for improvement between sectors.

Question 4b. How much will these legislatively-mandated activities by BITS members improve security?

Answer. While the mandates in the proposal may improve BITS members' cybersecurity practices, we see much of the potential improvement coming from enabling more voluntary collaboration. For example, as noted above, we would anticipate improved information sharing and consequently better collective security among multiple sectors, including financial services.

In closing, we reaffirm our commitment to addressing this critical issue, and thank the committee for its active engagement. Please feel free to contact me with any further questions or concerns.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR LARRY CLINTON

Question 1. Playing Devil's advocate, if critical infrastructure must be regulated, what do you think that regulations should look like?

What is an appropriate framework for regulations?

Answer. Although the ISA generally supports market incentives as opposed to Government regulation as the best way to spur the needed investment in cybersecurity, this is not an absolute.

In fact ISA has always advocated a multi-tiered system with appropriate regulation mixed with market incentives. This approach is developed more fully in the "The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 11th Congress" (2008) and the "Social Contract 2.0: A 21st Century Program for Effective Cyber Security" (2009)—both attached.

The key consideration is that cybersecurity is not simply an "IT" issue but an enterprise-wide risk management issue. If we are considering cybersecurity as a risk management issue we need to assess not only the technical considerations, but also the economic considerations. Research has consistently demonstrated that cost is the single biggest barrier to implementing effective cybersecurity standards, practices (see CSIS and Pricewaterhouse Coopers studies cited in my written testimony) and technologies which other research has demonstrated to work (see NSA testimony, PWC survey, and Verizon/Secret Service studies cited in my written testimony).

Where regulation is an inherent part of the economics of an industry, such as in many critical infrastructures (electricity, water, nuclear power etc. as well as some element of the financial system) than the traditional regulatory structures may be an effective tool for promoting appropriate investment in cybersecurity. Indeed in some industry sectors of great interest to cybersecurity policy makers regulation could be a more effective mechanism than a market incentive if, as in the case of water systems for example, there really is no market.

Of course many of these entities are regulated at the State and local, not Federal level. Moreover, as the decision making devolves to lower levels of Government more localized issues may evolve. For example a State PUC may be resistant to approving investments by a power company for fear of the effect this may have on local utility rates which could have political complications for members of the State commission. However the Federal Government has long history in finding ways to provide incentives to the States and localities to adopt policies in the National interest.

However even in some of these regulated sectors, market incentives may still be a better mechanism than regulation. The regulatory structure in most instances is too slow to keep up with the pace of cyber attack vectors which change with the speedy evolution of technology. Also regulation tends to push entities to achieve minimal compliance whereas we may need a more aggressive effort on the part of enterprises not just to comply with minimum standards but to affirmatively look for malware and cooperate with broad industry sectors, and possibly beyond in information-sharing activities (see paper on information sharing by Jeff Brown in the attached Social Contract 2.0).

For many of these sectors a more effective mechanism may well be the use of streamlined regulation wherein outdated provisions or redundant audit requirements could be offered in return for investment in more aggressive methods of cybersecurity including intensive internal monitoring of unauthorized outbound traffic and participation in creative and more modern models of information sharing than are currently being operated by DHS (see Brown paper cited above).

Question 2. We have had a public-private partnership for several years yet the cyber problem continues to grown, doesn't that indicate that the model doesn't work?

Answer. To begin with I'd suggest this is a non-sequitur. The reason the cyber problem has grown is not that the partnership has failed but because the current incentive structure massively favors the attackers. Cyber attacks are cheap, easy to acquire, and can generate massive profits. While cyber defense is a generation behind the attackers, it's difficult to justify ROI since metrics for prevented attacks are impossible to generate and cyber criminals are rarely caught.

Moreover, both the Cyber Space Policy Review and the most recent Verizon/Secret Service study have demonstrated that the market has already produced adequate mechanisms to prevent or stop most attacks which suggests the market is working (indeed most attacks are currently stopped—just too many still get through).

That said, the ISA has said from the first publication of the National Strategy to Secure Cyber Space (2002) that the missing link in the public-private partnership is the lack of incentives. The public-private partnership is the right model but it needs to be evolved to meet the modern threats and more fully implemented—especially by the Government partners.

Research cited above as well as in my written testimony has long demonstrated that that only a substantial minority (probably between 30% and 40%) of enterprises have what may be called a natural ROI for security investment. When such

as natural confluence occurs then private sector entities will make adequate security investment.

However, as illustrated in the pan-association White Paper on cybersecurity (cited in my written testimony and also attached) in most instances the public sector and private sector assess risk differently.

In short form, for most of the private sector security is simply an economic consideration. If you own a warehouse and 10% of your inventory is "walking out the back door" every month, you will not buy the cameras, hire the guards, etc. to solve your security problem if your study shows that it costs 11% to do so. That is a good risk management decision from a private-sector perspective.

The public sector has economic considerations, but also additional non-economic considerations (National security, privacy, politics etc.) and thus may have a lower-risk tolerance than their private partners because they simply assess risk differently.

However, as the trade associations who signed onto that paper have attested, we recognize that in an interconnected cyber world the private sector may be required to take on new, non-economic, and traditional public sector responsibilities with respect to cybersecurity.

Therefore the public-private partnership which has heretofore ignored the economic aspects of cybersecurity needs to evolve into a fuller and more sustainable model which includes Government finding ways to offset the non-economic investments it would like private industry to make in the interests of broad National security.

Additionally, the fact is that the public sector has not been faithful to following through on their responsibilities in the partnership as laid out both in the NIPP and the Cyber Space Policy Review. For example, markets cannot function without information—a central tenant of Wall Street—but it is well-acknowledged that despite millions spent on supposed Government information-sharing programs most such shared information is of little or no use to the private sector. Government still does not share the actionable threat information that would allow among other things for a proper assessment of cyber risk and assist greatly in making the proper investments.

Industry is not blameless here also. As illustrated in two additional volumes attached ("50 Questions Every CFO Should Ask About Cyber Security" and "The Financial Management of Cyber Risk") industry, largely due to antiquated corporate structures and misunderstandings about the true nature of the cyber threat tends to misunderstand the true financial implications they are dealing with.

These and other issues explain why the partnership has not fully worked are more extensively detailed in the pan-association white paper.

Question 3. Mr. Clinton, you advocate for the providing of market incentives to the private sector to improve cybersecurity, given the significant budget issues the Congress faces how can we afford to provide market incentives for cybersecurity to the private sector?

Answer. One of the most persistent problems with digital economics is that everyone wants to capture the profits of digital technology but resists reinvesting a small portion of these profits in securing the technology that is generating them.

Nearly every company in the world has by now factored into its business plan the wonders of digitalization—web-based marketing, international supply chains, VOIP instead of traditional telecommunications, and remote workers. Yet, as described above we are not getting the investment in cybersecurity that we should.

This is true for the Federal Government as well. For example the Obama administration has announced a "cloud first" strategy for the Federal electronic systems that they claim will save them between $20–50 billion a year. Some of that money ought to be being plowed back into system-wide—not just Government—cybersecurity.

However, assuming that none of this money will be invested in market incentives there are still many levers the Federal Government can use to generate more private cyber investment which require little or no Government spending. Ironically, many of these incentive structures are widely used in other areas of our economy; we simply have not yet applied them to cybersecurity.

The key is to reduce Government-induced costs on industry, rather than provide direct Government subsidies such as with tax incentives.

For example many companies may be attracted to making greater cybersecurity investments in return for lower liability. Less stringent liability costs the Government nothing but cold be perceived as an economic benefit to industry.

Another example is streamlined regulations, or as appropriate accelerated permitting and approvals. For example many enterprises are buckling under redundant cybersecurity auditing requirements. If the Government could develop a sound base-

line audit to simply remove the redundancy this could be offered as a carrot to enterprises that demonstrate investment in proven effective e-cybersecurity techniques such as those identified in the Verizon/Secret Service study cited in my testimony.

On a broader scale there are numerous outdated analogue-based laws (see Cyber Space Policy Review Appendix A) which could be modified possible with reduced cost to industry.

Government procurement—not just for IT equipment—could also be tied to more stringent cybersecurity on the part of firms that compete for Government contracts, or access existing (not additional) Government spending programs (e.g. small business loans—and all the TARP money should have come with cybersecurity requirements). In these cases we are not talking about Government spending more, we are simply talking about who gets the spending the Government is making—weigh it more heavily in terms of the compelling National interest of cybersecurity. No new spending required.

There is also a great deal that can be done to stimulate the cyber insurance market. With a broader insurance market we can off-load much current Government risk to the private sector. Moreover, insurance (discounts) are a major motivator of all sorts of pro-social behavior from smoking reduction to improved driving and building safety. ISA has done a fair amount of work on how to use insurance better ranging from some relatively immediate items such as sharing information leading to lower rates and greater uptake (due to more realistic risk assessments and pricing) to broader programs dealing with National re-insurance.

The Social Contract documents (attached) provide some additional examples.

Question 4. If as you say we know how to prevent or mitigate most basic cyber attacks by use of current standards and activities why don't we just mandate that companies do these best practices?

Answer. We can't just put seatbelts on the internet and think we have solved the problem.

As identified in answer No. 2, the problem is that there are massive incentives right now favoring the attackers.

Yes we have come up with ways to deal with most current attacks, but the attack methods will continually evolve.

ISA is not interested in solutions; it is interested in creating a sustainable system of cybersecurity.

To do this we need a much more dynamic motivator than Government regulations, we need to use the market.

As described in greater detail in Chapter 1 of each of the Cyber Social Contract documents attached, the Government regulatory model invented to address the hot technology of 2 centuries ago—the railroads—is not going to work for the 21st Century problem of cybersecurity. We need a more active model which will keep up with attacks, can be applied internationally, will not provide a roadmap to the attackers and generate an atmosphere of foe compliance (equivalent to campaign finance laws which everyone complies with and no one thinks actually addresses the "problem" they are supposed to solve).

Regulations, (outside of those sectors for which the regulations are part of the inherent economy of the sector as described in answer 1) will be too slow, outdated quickly, and too minimalistic to address the modern problem we face.

Question 5. If companies are losing so much money due to cyber attacks, why are there not already enough incentives for them to invest to stop the attacks?

Answer. Part of this answer was addressed in the answer to question 3, above, where we discussed the fact that industry and the Government assess risk in fundamentally different ways with industry, concerned almost entirely about the economics of the situation, have a greater risk tolerance than the public sector.

However there are many other problems. For example, it is very hard to make truly accurate assessments of economic cyber losses for a variety of reasons including the fact that for sophisticated cyber attacks one may not know they have been the victim of the attack until long after it has occurred because as in the case of the loss of corporate IP, (the largest economic loss) the property is not stolen in the physical since—it remains—it's just a copy has been made and maybe being used to create a clone product or service.

In still another complication we have the "interconnection problem". Due to the inherent interconnectedness of the internet it is possible for a thief to steal your data that happens to be residing on my system (I may not even have a direct relationship with you—I could be a sub-contractor to a subcontractor—with little or no incentive to protect your data which is valuable whereas my own data may not be as valuable so I don't invest in security adequate to your needs.

Additionally, we have the problem with poor appreciation of actual financial risk as described above.

Finally, there is the fact that in the current economic climate business are being forced to make themselves ever more efficient including cutting costs by adopting less secure technologies. VOIP, international supply chains and cloud computing are all examples of technologies that are increasing our cyber risks but are being widely deployed (including by the U.S. Federal Government) despite their security flaws due to the irresistible economic imperatives we all face.

Government's job ought not to be to punish the victims of cyber attacks who are forced to compete in the digital world we now inhabit but to use the mechanisms at its disposal creatively, as described above to assist enterprises in securing our Nation's system in a sustainable and economically sensible way.