S. HRG. 112–886

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 21, 2011

Serial No. J–112–29

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
88–182 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON CRIME AND TERRORISM

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

HERB KOHL, Wisconsin	JON KYL, Arizona
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
AMY KLOBUCHAR, Minnesota	LINDSEY GRAHAM, South Carolina
CHRISTOPHER A. COONS, Delaware	

STEPHEN LILLEY, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

ANSWERS

SUBMISSIONS FOR THE RECORD

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

TUESDAY, JUNE 21, 2011

U.S. SENATE,
SUBCOMMITTEE ON CRIME AND TERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 2:38 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, Chairman of the Subcommittee, presiding.

Present: Senators Whitehouse, Leahy, Klobuchar, Coons, and Blumenthal.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Senator WHITEHOUSE. All right. The hearing will come to order. I understand that Congressman Langevin is nearby, and I have been waiting for him to be nearby. And what I think I will do in terms of order of proceeding is to give my opening statement, invite Senator Blumenthal to give an opening statement, invite anybody else who joins the hearing to give an opening statement, and then call on Congressman Langevin, who by then should be here.

I want to note that it has been a real pleasure to work on this issue with the Ranking Member, Senator Jon Kyl. He cannot be here today for the best of reasons. He is up at the White House in the debt limit negotiations. As important as this hearing is, I do not think it tops being at the White House and the debt limit negotiations. He has been great to work with, and this is an important issue to him, and we have worked on legislation together, so I just want to make it a matter of record that he has been a thoughtful and helpful colleague in these discussions.

The hearing that brings us together today returns to a topic of vital importance: our Nation's cybersecurity. Since the Subcommittee's hearing back in April, the news has been full of reports of hacks and cyber intrusions. Lockheed Martin, Sony, Epsilon, Sega, the International Monetary Fund, and the Web sites of the CIA and the Senate, to name just a few, have been compromised in just a two-month period. This reflects the fact that our Nation's privacy, intellectual property, and security are under constant and worsening cyber attack.

The Internet age has brought with it an explosion of new commerce, freedom of expression, and economic opportunity. We see its benefits at home and around the world. Unfortunately, our increased connectivity allows criminals, terrorists, and hostile na-

tions to exploit cyberspace, to attack America, invade our privacy, loot our intellectual property, and expose America's core infrastructure to cyber sabotage. Whether by copying source code, by industrial espionage of military product designs, by identity theft, by online piracy, or by outright stealing from banks, cyber crime cripples American innovation and commerce, kills jobs, and undermines our economic and national security.

Congress must act to provide the administration as well as private entities the tools and authorities they need to improve our Nation's cybersecurity. To that end, I am very glad that the administration has weighed in with its legislative proposals to improve our Nation's cybersecurity. The administration proposals aim at key cybersecurity challenges, for instance, securing our critical infrastructure, such as our electric grid, and providing for voluntary assistance and response to a cyber incident.

I am glad that the Subcommittee will have the opportunity to hear from the administration today, and I am happy to welcome our witnesses from the Department of Justice, the Department of Homeland Security, and the Department of Commerce.

I am also very glad to be welcoming Congressman Jim Langevin of my home State—boy, his timing is good. He just came through the door as I said that—to the Committee. Congressman Langevin is a well-regarded leader on cybersecurity, having served on the House Intelligence Committee, led the Congressional Cybersecurity Caucus, and co-chaired the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. I very much look forward to his testimony and appreciate his friendship.

Our hearing today will focus on three elements of the administration's proposals that fall within the Judiciary Committee's jurisdiction and expertise: the data breach section, the voluntary information-sharing proposal, and recommendations for increased criminal penalties under the hacking statute, 18 United States Code Section 1030.

This Committee is well situated to consider those questions, particularly in light of the longstanding leadership of Chairman Leahy on these issues. I look forward to working with the Chairman, with Senator Kyl, and other Members of this Committee as the Senate prepares cybersecurity legislation.

The three proposals we will focus on today are central to any discussion of improved cybersecurity and individual privacy. The recent data breaches at Sony, Epsilon, and Sega reveal how determined criminals can compromise Americans' privacy and economic security. Prompt and clear notification of such a breach is important to enable Americans to limit the damage caused by data breaches and resulting identity theft.

Today a confusing patchwork of state laws provides for different notifications to different customers across the country, delaying and raising the cost of breach notification. The administration would replace this patchwork of State laws with a single federal standard: requiring notification of a breach to the Department of Homeland Security, which would then pass on the information to the Federal Trade Commission, the Secret Service, and the FBI for appropriate enforcement actions.

Proper sharing of cybersecurity threat information also is vital. The administration has recommended, subject to various safeguards, enhanced sharing of cybersecurity threat information between private industry and the government. The administration also has recommended enhancing criminal penalties for hackers. Our current laws have proven to lack appropriate deterrent effect.

This hearing will consider the need for stiffer penalties for hackers who harm our privacy, our National security, and our economic well-being. Stiffer penalties, I would note, are of little use without adequate law enforcement resources to impose them. I would note further that this is an area where civil actions by the government to protect the public, such as the government's recent action in the Coreflood Botnet, are particularly important.

I am glad that we have the opportunity to evaluate the administration's proposals today. We have witnesses joining us from the Department of Justice, the Department of Homeland Security, and the Department of Commerce. I thank them for being with us today and for their ongoing work to secure cyberspace.

I would also briefly note that I believe that the Senate should consider issues beyond the current scope of the administration's proposals, such as increasing public awareness of cybersecurity threats, improving industry self-defense, developing rules of the road for our information highways, improving supply chain security, considering secure domains for critical infrastructure like the electric grid, increasing cyber resources within the Government, and strengthening cyber research and development.

I look forward to working with the administration and my colleagues on each of these important issues as we strive to strengthen our Nation's cybersecurity.

Before I recognize Congressman Langevin, Senator Blumenthal, would you like to make a statement?

STATEMENT OF HON. RICHARD BLUMENTHAL, A U.S. SENATOR FROM THE STATE OF CONNECTICUT

Senator BLUMENTHAL. A very brief statement. Thank you, Senator Whitehouse, Mr. Chairman. Thank you for your work on this issue, which has been continuing not only in hearings but in many other arenas and forums, and thank you to the Chairman of the Judiciary Committee, Senator Leahy, for his leadership. And welcome, Congressman. Thank you for being here. And to the administration, I appreciate not only your being here but the very constructive and important proposals that you have made in many of these areas.

Senator Whitehouse has articulated many of my own concerns that arise from the real and present danger that cyber attack reflects. My own view is that America's next 9/11 may well be a cyber attack, and I am paraphrasing when I say that the soon-to-be-confirmed Secretary of Defense, Leon Panetta, who in the hearing said America's next Pearl Harbor is likely to be a cyber attack.

For consumers, of course, the danger is very much real and present because they entrust companies like Sony or Citigroup with very sensitive and personal information, which could do grave harm to them if it is hacked or improperly used or lost, and we have seen all occur in recent months and years.

Let me just say that I appreciate the administration's proposal that notification occur in the case of breaches that carry, and I am quoting, "a significant risk of harm." I believe the notification has to be broader, and I believe that there are principles that have to be included: notification as soon as possible by mail, phone, or email, or all of them; a second notification that clearly indicates whether the breach compromised any consumer information; third, notification that is provided without unreasonable delay so long a law enforcement authorities do not require that notification—and I mean explicitly require that notification—be delayed for investigative purposes. And I will be interested to know whether the witnesses agree with those principles.

I also believe, as Senator Whitehouse articulated very well, both of being former law enforcement officials, that indeed law enforcement is critical here and that the government cannot be expected or relied upon to do it all. I happen to believe that there ought to be a private right of action, and I will be interested to know whether the witnesses agree that citizens who are potentially harmed, who can show damages, should be able themselves to go to court and seek remedies.

And, finally, I believe that remedies should be greatly enhanced. There is a very real need for stronger, more effective remedies to help mitigate any ongoing damage as well as provide relief for people who are actually harmed.

So thank you, Senator Whitehouse, for giving me this opportunity to begin.

Senator WHITEHOUSE. Thank you, Senator Blumenthal.

It is now my great pleasure and privilege to recognize my friend and colleague, Congressman Langevin, who has represented the Second Congressional District of my home State of Rhode Island since 2000. During that time, he has emerged as a well-regarded leader on cybersecurity. He serves on the House Intelligence Committee. He led the Congressional Cybersecurity Caucus. He cochaired the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. He has introduced important cybersecurity legislation in the House, and he has convened an important meeting at our university at home, the University of Rhode Island, at which General Alexander, the commander both of NSA and Cyber Command, attended and spoke. It is not often we get four-star generals in Rhode Island, so that was a memorable day organized by Congressman Langevin.

Before being elected to the House, Congressman Langevin was the secretary of state for Rhode Island and a member of the Rhode Island House of Representatives. He is a graduate of Rhode Island College and earned a master's degree in public administration from the Kennedy School of Government at Harvard University.

We are delighted to have you here, Congressman Langevin. Please proceed.

STATEMENT OF HON. JIM LANGEVIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF RHODE ISLAND

Representative LANGEVIN. Chairman Whitehouse, thank you very much for the introduction, the welcome, and the opportunity to speak today. Before I begin my prepared remarks, let me just

thank you for your leadership on this very important issue of cybersecurity. Your partnership and leadership on this issue have been invaluable to me, deeply appreciated both in the work we have done on this issue back in Rhode Island, but nationally here in the Congress, and particularly your experience as a former Attorney General and U.S. Attorney have been very insightful and, again, invaluable, and especially your work when you were on the Senate Intelligence Committee. So, again, I could not have done a lot of the work I have done without your leadership and support, and I am very grateful for your work.

I would like to thank you, Chairman Whitehouse and Ranking Member Kyl and Senator Blumenthal, for inviting me to testify today on one of the most critical national security challenges facing our contractor today. Cyber incidents have grabbed headlines in recent months, with our top companies seeing intrusions and loss of data and our constituents are beginning to realize that the Internet is a highly contested space where personal information is never truly secure.

The common thread is that these threats all take advantage of our strong reliance on the Internet for social communications, business, and national defense, and the damage will only increase as that reliance grows.

The first crisis that we are facing, of course, is highly skilled cybersecurity professionals. Our Nation is a leader in Internet security technology, but we do not have enough highly trained individuals to match our growing needs. In Rhode Island, we are working to educate our future workforce for the 21st century cybersecurity jobs through programs like developing a statewide Cyber Center of Excellence that will cultivate cyber talent in our State while meeting the increasing need for a strong public-private relationship in cyberspace.

We must also align our laws and policies with the realities of today's Internet, and I appreciate the administration's proposal to move in this direction. The foundations of trust and known identity upon which the Internet was built have enabled criminals to take advantage of those using the Internet for legitimate commerce. Organized crime, of course, is fully operational online, stealing billions of dollars every year to support worldwide networks of crime, yet RICO laws do not apply in cyberspace. The administration has proposed allowing RICO to cover crimes committed in cyberspace as well as setting mandatory minimum sentences for intrusions into critical infrastructure.

Similarly, recent incidents, such as the Sony and Citibank intrusions, have highlighted large discrepancies in our data breach laws. Currently each State regulates when and how a company should disclose a breach of customer data and those affected. This regime makes little sense in cyberspace where crimes and transactions take place at a national or international level. The administration's proposals, as well as those introduced in the House and Senate, seek to set a federal standard. As we move to this model, however, we must also take care to implement the most effective, not the lowest, standard for reporting.

Finally, we must reexamine new opportunities for voluntary information sharing to ensure that we stop new threats before they

reach their target. Today government, businesses, and citizens all build their own digital fortifications and hope they as positioned to stop the right threat.

Now, while the problem of attribution in cyberspace is always an issue, the government has a sophisticated understanding of what the various threats look like. It also currently lacks the visibility of the private sector, telecommunications in particular, which can better pinpoint the source of the threat or even stop it before it reaches our digital doorstep. Rather than protecting our citizens, we are actually losing the ability to stop attacks before they take place and provide better data security for everyone.

To address this issue without compromising individual privacy, the administration proposes allowing cyber threat information to be shared voluntarily with the Department of Homeland Security so that businesses, private citizens, and the Government can all benefit from and be better protected by the increased capabilities and insight of an enhanced public-private partnership.

For this arrangement to work, of course, we must institute strict oversight to ensure that no personal communications or sensitive data are inappropriately shared with the government by businesses. If done correctly, this could greatly enhance privacy by stopping malicious intrusions or large data theft efforts and would provide a clearer picture of the health and the security of the Internet.

Mr. Chairman, I will stop there but, of course, invite you to consider the longer statement that I am submitting for the record. We must implement sensible policies that enhance our security and our privacy before a serious cyber incident leads to decisions that could fundamentally alter one of the most incredible tools of our time.

I want to just conclude by, again, commending you, Senator Whitehouse, for being a true leader on this issue. Again, as a former Member of the Senate Intelligence Community and Chairman of this Subcommittee, I appreciate the great work that you are doing. Thank you, Mr. Chairman, Ranking Member Kyl, and Senator Blumenthal, for this opportunity, and I certainly look forward to working with you to make the Internet a stronger, more secure domain for all.

[The prepared statement of Representative Langevin appears as a submission for the record.]

Senator WHITEHOUSE. Well, thank you, Congressman Langevin.

First, your longer statement will, without objection, be part of the record of this hearing, and I appreciate the thought and care that you put into it. And I look forward to continuing to work with you as this goes forward. Your interest and expertise in this issue, your leadership on this issue, are recognized on this side of the Capitol, and clearly you have taken considerable trouble to come over here and join us on the Senate side today. So we appreciate it very much. I know that important business calls you back to the House, so we will excuse you at this time with much appreciation for your trouble today and for the content of your testimony.

Representative LANGEVIN. Thank you, Mr. Chairman.

Senator WHITEHOUSE. All right. We will now call up the administration witnesses.

There is a statement that we have that is, I gather, a joint statement. Do the three of you adopt it as your testimony to this Committee?

Mr. BAKER. That is correct, Senator, yes. We ask that it be made part of the record.

Senator WHITEHOUSE. Okay, so that is yes, yes, and yes for the three witnesses, may the record reflect. And I understand that each of you would like to make a separate oral statement before we get into questions and answers. Is that correct? All right. Well, why don't we proceed across the line. It turns out to be alphabetical order as well, but we will start with Jim Baker.

Jim Baker currently serves as an Associate Deputy Attorney General at the U.S. Department of Justice where he is responsible for a wide range of national security, cybersecurity, and other matters. Mr. Baker previously served as Counsel for Intelligence Policy at the Department from 2001 to 2007 where, among other things, he was in charge of representing the United States before the Foreign Intelligence Surveillance Court. From 2008 to 2009, Mr. Baker was assistant general counsel for National Security at Verizon Business. He has also taught national security law at Harvard Law School and been a fellow at the Institute of Politics at Harvard's Kennedy School of Government.

Mr. Baker, please proceed.

STATEMENT OF JAMES A. BAKER, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. BAKER. Thank you, Mr. Chairman, Members of the Committee. Thank you for the opportunity to testify today before you today on the administration's cyber legislative proposal.

Mr. Chairman, as you have noted and as everyone else has noted so far today, the Nation faces a dangerous and persistent cyber threat. As we all know, we rely heavily on the Internet to conduct our most important activities. Information technology has become the nervous system of the country, and today that system is highly vulnerable to exploitation and attack.

More importantly, malicious actors know this. Recent publicly disclosed cyber intrusions reflect the breadth and intensity of the efforts by malicious actors to exploit existing vulnerabilities and infiltrate and compromise our networks. Such actions threaten those networks, the data they contain, and the critical infrastructure systems that rely upon them. Every day information systems in the United States are compromised, and criminals and other malicious actors steal significant quantities of intellectual property and money.

Over the past several years, the Federal Government has worked to improve the security of its own networks by, for example, reducing the number of Internet connections that the departments and agencies use, implementing the EINSTEIN program, and enhancing information sharing and coordination with our international partners.

In addition, we recently launched a pilot program to improve the security of key defense industrial base companies. We have also urged private citizens to improve the security of their own com-

puters by installing software updates promptly and using updated anti-virus programs.

As we go forward, it is critical that the American people understand that when our cyber defenses are not successful at preventing an intrusion, many of the mechanisms that malicious actors use to steal from us could allow them to disrupt or damage our data and our infrastructure. Malicious actors could, for example, interfere with our ability to communicate effectively by misrouting emails; they could also divert aircraft containing passengers and military equipment; they could delete medical information on hospital computers; and they could shut down transportation systems and the electric grid.

Malicious actors attempt to exploit the vulnerabilities of our information systems to compromise them at the hardware, software, and firmware levels. They try to establish a persistent presence in our networks, using system administrators' authorities that they have purloined, in a manner that makes them difficult to detect and virtually impossible to eradicate. Even if we build firewalls and have air gaps around networks to protect those systems from known malware, there are still ways to get in.

Anti-virus and other perimeter-based malware detection and prevention systems cannot detect and stop malware that no one has seen before, and malicious actors develop new malware continually. This is known as the Zero Day threat.

Moreover, firewalls and air gaps do not protect against the insider threat. Employees or other insiders could, intentionally or inadvertently, introduce malware into our networks using a compromised thumb drive, for example, on a protected network or connecting a computer from a protected network to the Internet. In addition, our adversaries compromise our information by installing software, hardware, and firmware already containing vulnerabilities in the products that we use while those products are being manufactured. This is the supply chain threat.

All of this emphasizes the need for us to develop effective cybersecurity solutions that account for the fact that frequently we will have to use networks that may be compromised. We will have to learn how to operate successfully in a degraded cybersecurity environment.

Mr. Chairman, we must be candid about these risks. For example, private entities must do a better job of informing their customers and their shareholders about the losses they suffer and the vulnerabilities that they face, including the problems that exist with the products that they bring to market. Government must, for example, act purposefully and with dispatch to improve the security of its own networks.

Several of the administration's legislative proposals are intended to enhance our ability to protect the American people. Our data breach proposal, for example, as several have noted, would establish a uniform national standard for certain entities that suffer a data breach to require them to timely report such breaches to the customers and to law enforcement. Other proposals would enhance and harmonize penalties for cyber offenses such as causing damage to critical infrastructure computers. The administration's proposal is a first step in addressing these challenges. We look forward to

working with Congress on a bipartisan basis to improve and amplify this proposal.

As we move forward, whatever we do to enhance security, we must ensure that we establish adequate oversight mechanisms and appropriate privacy protections to safeguard the civil liberties of all Americans. We must also ensure that we foster innovation in this vibrant sector of our economy.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you, Associate Deputy Attorney General Baker. We, too, look forward to working with the Department of Justice, to use your words, to improve and amplify the administration's proposals. You have always been wonderful to work with, and we have great pride in the public service that you have given to this country over many years. It is not an easy thing. You have had many late and difficult nights and a lot of worries. I know a little something about those FISA Court proceedings, so I know how burdensome that has been, and I know you are joined by your son and your daughter today, and in front of Julian and Hadley, I just wanted to say those words about you because I am sure that there were times with them that you missed because of the press of your responsibilities, and I am happy to take this occasion to let them know how important what you do for your country is.

And now I would like to turn to the Chairman of the Judiciary Committee, the distinguished Senator Pat Leahy. I will offer him a chance to give opening remarks.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Well, thank you very much. Incidentally, I concur with what you just said about Mr. Baker, and I wanted his family to hear that, too. You know from your own work on the Intelligence Committee and I from this Committee, how much work can go into some of those things. Some of the times you are going to be working, you come home and the family says, "What were you doing?" you say, "Cannot tell you." So I commend you for that.

Chairman Whitehouse, I commend you for your work on the Subcommittee on Crime and Terrorism. This whole idea of developing a comprehensive strategy for cybersecurity—we will talk about nuclear weapons, we will talk about this, that, and the other thing—but I think this is probably one of the greatest challenges facing our country today.

Look at some of the major data breaches: Sony, Epsilon, RSA, the International Monetary Fund, and Lockheed Martin. That is just naming a few. I have often talked about what happens in a part of the world like where I come from, in the Northeast, when it is the middle of January and it is 10 or 15 degrees below zero, and a cyber terrorist closes down all our power grids. I mean, these are major concerns.

Our government computer networks have not been spared. We see it at the CIA. We saw it here in the Senate. The Department of Defense tells us they have attacks on them all the time. So I think protecting America's privacy but also our security and cyberspace is a top priority for this Committee.

We are working with the Obama administration and others in Congress to develop a comprehensive national strategy for cybersecurity. I reintroduced my Personal Data Privacy and Security Act to establish a national standard for data breach notification and to require that companies protect our sensitive personal information. If somebody broke into your house and stole all your papers, you would want to know about it. Well, if they break into a company that holds all your medical records, your tax records, and everything else, you ought to know about it.

In a few weeks, I will include this bill in the Committee's business agenda so we can report the legislation again. It has had strong bipartisan support before. I hope that it will again.

Today, having the Departments of Justice, Commerce, and Homeland Security here, it is important that we hear from you. This is not a Democratic or Republican issue. It is one where we want to protect our own personal privacy and liberties, but we also want to protect the country. And I think it can be done, but it is going to need a lot of expertise and work.

Senator Whitehouse, I commend you for holding the hearing, and I am glad we are doing this.

[The prepared statement of Senator Patrick Leahy appears as a submission for the record.]

Senator WHITEHOUSE. Well, thank you, Chairman. I appreciate your leadership in this and so many other issues.

We will now go on to our next witness, from the Department of Homeland Security, Greg Schaffer. He is the Acting Deputy Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security. Mr. Schaffer previously served as Assistant Secretary for Cybersecurity and Communications where he led the coordinated efforts of CS&C and its components, including the National Cybersecurity Division, the Office of Emergency Communications, and the National Communications System. Mr. Schaffer previously held positions at Alltel Communication, LLC, and PricewaterhouseCoopers as well as in the Computer Crime and Intellectual Property Section at the U.S. Department of Justice.

We are glad to have you with us, Mr. Schaffer. Please proceed.

STATEMENT OF GREG SCHAFFER, ACTING DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. SCHAFFER. Thank you, Chairman Whitehouse, Chairman Leahy, and distinguished Members of the Subcommittee. I appreciate the opportunity to speak to you today about what we all seem to believe is a critically important security issue for our country.

I will not reiterate the threat situation that has been clearly stated by Mr. Baker and the Members of the Committee, but I will say that the theft of intellectual property both from the government and from private sector entities does pose a serious risk to our country's economic viability and our security. What is worse is that the connectivity of industrial controls creates a situation where there is an ability to take things even farther. To disrupt the delivery of power, the delivery of transportation services, our finan-

cial services sector, all can be interrupted by hackers who can reach us from anywhere on the globe. These are national security, homeland security, and economic security issues that really can only be addressed through the efforts of our entire society. Both government, industry, and even individual citizens will have to play a role in solving these problems.

The legislative proposal that the administration has put forward clarifies the authorities of various departments in a variety of ways. It moves to enhance the collaboration with industry, and it drives for outcomes and progress in reducing risk in a variety of ways. The proposal clarifies that the Department of Homeland Security leads the protection of federal civilian networks, and it clarifies our authority to do so with the private sector by providing a variety of voluntary services as well as capabilities that the private sector needs from government.

It also presents an opportunity to modernize the Federal Information Security Management Act, as many bills that have been presented over the last several years have tried to do, to move away from a paper compliance exercise and in the direction of continuous monitoring and operational improvement and reduction of risk for federal departments and agencies.

In the area of personnel authorities, the proposal is designed to give DHS the kind of flexibility that the Department of Defense already has in order to compete in a market that is highly competitive for a very small number of highly skilled individuals. While we will never in government pay the same as some of our competitors for staff in the private sector, we do need the ability to rise to the level of others in the Federal Government.

With respect to protecting critical infrastructure, the bill has both voluntary and mandatory provisions. The administration's proposal clarifies the authority to provide assistance on request to private sector entities, including alerts and warnings, risk assessments, onsite technical support, and incident response. Our ability to provide those services is clarified so that we do not have any confusion by the private sector in terms of what we can do for them in a difficult moment.

From an information-sharing perspective, the proposal removes many of the barriers between government and industry. In particular, uncertainty slows us down. When industry is unclear about whether or not they can share information, several days of working with lawyers for clarity can delay the ability to deliver capability and defensive measures. This would provide immunity when industry is sharing with government in order to allow that to happen much more quickly and allow us to do this in a way that is, nonetheless, consistent with robust oversight for privacy, civil liberties, and indeed criminal penalties in the event of a violation of procedures that would be established to control how that information would be taken in.

Under mandatory provisions, the proposal allows through a rulemaking process for Government to work with industry to establish who is in the most critical of critical infrastructure and for those entities to work with us to establish risks that need to be mitigated and then frameworks that can be used to mitigate those risks.

Through that process and the development of plans by industry under those frameworks, we believe using transparency we can significantly reduce the amount of risk within the private sector.

The proposal really builds on many proposals that have appeared in bills that the Congress has put forward. It builds on those proposals over the last several years, and we are anxious to work with you. It is the beginning of a process in the discussion of these proposals and others that have been suggested, and the administration is very anxious to work with you as this moves through the Congress.

Thank you.

Senator WHITEHOUSE. Thank you very much, Mr. Schaffer.

Our final witness is Ari Schwartz. He serves as the Senior Internet Policy Advisor for the Information Technology Laboratory at the National Institute of Standards and Technology, which is within the Department of Commerce. He represents NIST on the Department of Commerce Internet Policy Task Force, providing input on areas such as cybersecurity, privacy, and identity management. Mr. Schwartz came to NIST in 2010 after serving almost 13 years as vice president and chief operating officer of the Center for Democracy and Technology, where he focused on increasing individual control over personal and public information.

Good to have you with us, Mr. Schwartz. Please proceed.

STATEMENT OF ARI SCHWARTZ, SENIOR INTERNET POLICY ADVISOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U.S. DEPARTMENT OF COMMERCE, WASHINGTON, DC

Mr. Schwartz. Thank you, Mr. Chairman.

Chairman Whitehouse, Chairman Leahy, Members of the Committee, thank you for inviting me to testify today on behalf of the Department of Commerce on the administration's cybersecurity legislative proposal.

The main goal of this proposal is to maximize the country's effectiveness in protecting the security of key critical infrastructure networks and systems that rely on the Internet while also minimizing regulatory burden on the entities that it covers and protecting the privacy and civil liberties of the public.

I will address three relevant parts of the proposal: first, creating security plans for covered critical infrastructure; second, data breach reporting; and, finally, privacy protections.

First, on security plans, one important theme of the proposal is accountability through disclosure. In requiring creation of security plans, the administration is promoting use of private sector expertise and innovation over top-down government regulation. Importantly, the proposal only covers the core critical infrastructure as it relates to cybersecurity. DHS would define these sectors through an open public rulemaking process.

The covered critical infrastructure entities will then take the lead in developing frameworks of performance standards for mitigating identified cybersecurity risks and could ask NIST to work with them to help create security frameworks. There will be strong incentive for both industry to build effective frameworks and for DHS to approve those created by industry. The entities involved

will want the certainty of knowing that their approach has been approved, and DHS will benefit from knowing that it will not need to invest in the resource-intensive approach of developing a government-mandated framework unless industry really fails to act.

Covered critical infrastructure firms and their executives will then have to sign off on their cybersecurity plans, subject them to performance evaluation, and disclose them in annual reports. Rather than substituting the government's judgments for private firms', the plan holds the covered entities accountable to consumers and the market. This encourages innovation and mitigation strategies as well as improving adherence to best practices by facilitating greater transparency, understanding, and collaboration. The main goal is to create an institutional culture in which cybersecurity is part of the everyday practice without creating a slow-moving regulatory structure.

In our recently released green paper, the Department of Commerce has begun to further clarify major functions and services that would not be considered covered critical infrastructure under the administration proposal. We believe that the non-covered entities should develop the voluntary equivalent of the frameworks that are in the administration proposal that could begin to serve as the rules of the road for these companies that rely on the Internet similar to those that the Chairman suggested in his opening remarks. We are receiving comments on that paper until August 1st.

On data breach reporting, the administration has learned a good deal from the States, selecting and augmenting those strategies and practices that we felt most effective to protect security and privacy. The legislation will help build certainty and trust in the marketplace by making it easier for consumers to understand the data breach notices they receive and why they are receiving them, and as a result will better be able to take appropriate action.

As Secretary Locke and others at the Commerce Department have heard from many of the companies in different industries, including in response to our notice of inquiry last year, a nationwide standard for data breach notification will make compliance much easier for the wide range of businesses that today must follow 47 different legal standards.

Finally, I would like to point out that many of the new and augmented authorities in this package are governed by a new privacy framework for government that we believe would enhance privacy protections for information collected and shared with the government for cybersecurity purposes. This framework would be created by DHS in consultation with privacy and civil liberties experts and the Attorney General, subject to regular reports by the DOJ Privacy Office, and overseen by the independent Privacy and Civil Liberties Oversight Board. Government violations of this framework would be subject to both criminal and financial penalties.

Thank you again for holding this important hearing. I look forward to your questions.

[The prepared statement of Messrs. Baker, Schaffer, and Schwartz appears as a submission for the record.]

Senator WHITEHOUSE. Thank you.

Before I get into questions, let me just make one general point, because we are going to spend a lot of time working through this

together in the coming months. I am worried about the extent of the threat that we are facing right now and the time that it will take to work through some of the administrative procedures that are built into the administration's proposal. It seems to me that, to the extent that we can reach agreement and try to draw some of those bright lines forward and into legislation so that people can begin to rely on them and gain their protections more rapidly, that would be to our advantage.

I spent three years, if I recall correctly, just trying to get the Drug Enforcement Administration to knock off its ban on prescribed pharmaceuticals being prescribed electronically, and I had the support of the Department of Health and Human Services through all of that, and ultimately of the Attorney General. So when that is the pace of something that the government agrees with, it makes me concerned about the prospect of delay. So that is just an overall point about the reliance of the proposal on the administrative process. I think where we find agreement we should move things up.

In terms of defining these things, let me ask right off the bat: Are independent service providers on the Internet covered entities? And is the Internet itself and the provision of service across the Internet critical infrastructure within the definition as contemplated by the administration?

Mr. BAKER. Thank you, Senator, and I understand completely your first point about trying to move expeditiously through these things. I have been through a number of different efforts to write policies and procedures, and I agree, wherever possible, if we move them into statute, that would be fine, as long as we maintain the flexibility that we need to deal with the evolving threat.

But with respect to critical infrastructure, I will defer to my colleagues here, but I think there are different definitions of critical infrastructure as you move through the proposals. And just to highlight for folks, the different proposals are focused on achieving different things, and in particular, the proposal to modify the *Computer Fraud and Abuse Act* and add a prohibition on damaging or attempting to damage critical infrastructure. That has got a very——

Senator WHITEHOUSE. I am referring to the part that Mr. Schwartz was discussing in which the industries defined, I think in the language, as covered entities that are deemed to have critical infrastructure have to come in, generate their own plans, seek their approval, and if they are adequate, then they go forward. And that is the process by which we protect our so-called critical infrastructure. Are the ISPs critical infrastructure within that definition?

Mr. SCHAFFER. Senator, thank you for the question. I think that the proposal lays out some criteria and contemplates a rulemaking. But at the end of the day, I do think that the ISPs, being critical to connectivity for a wide range of entities and, therefore, likely to cause cascading effects if there is an outage within their infrastructure, would likely fall within critical. But, again, there would be a process in order to get to that under the current proposal.

Senator WHITEHOUSE. Well, that goes back to my opening problem, that we do not get around to even defining who the partici-

pants are in the protection of our critical infrastructure for some considerable period of time and some considerable effort in administrative rulemaking. But you all agree that in terms of going forward we in Congress should presume that the administration intends the ISPs to be in that process, and we can more or less deem them to be critical infrastructure in terms of working with them to beef up the security of the Internet.

Mr. SCHWARTZ. I would just have a little bit further of a discussion and discuss how we can start moving some of this further a little bit more quickly.

In terms of who is covered and how they are covered, one thing that we focus on in our green paper is the coverage of functions and services. So there are some things that ISPs do, and certainly large ISPs, that we may all consider covered. But there might be other functions and services that we do not consider covered. Maybe they do not meet the *PATRIOT Act* definition of what critical infrastructure is, perhaps even——

Senator WHITEHOUSE. Let us talk for a minute about—I think it was your testimony—actually, I take it back. It was Mr. Baker's—about needing to encourage consumers to be more aware and to take basic steps to protect their own computers and to protect the computers of those they link with from having malware that they host propagated into other people's computers. That is a pretty important thing to do. We have heard testimony that, you know, 80 to 90 percent of the threat out there can be blocked with commercial off-the-shelf technology if it were only used by people.

Mr. SCHWARTZ. Correct.

Senator WHITEHOUSE. So the ISPs are in a unique position because they are aware of the traffic coming through, know that your computer—in a way that you would never have a reason to know as an ordinary consumer—is infected with malware or is slaved to a botnet, and the terms on which the ISPs would deal with the consumer, where the consumer has been determined to be an unwitting sponsor, if you will, of a cyber threat. Where does that relationship between the ISP and the consumer with respect to the consumer's unwitting and unwilling role as a vector for a cyber threat get addressed in this legislation? Is that part of the cyber infrastructure?

Mr. SCHWARTZ. I will leave it to DHS to discuss what is covered and what is not covered in that way, but I will say, just to follow up on where I was going when I was raising what we cover in the green paper, that there are things that we know today, as you said, there are strong best practices, evolving standards that are out there today that we know will solve, as you said and as many experts that we have spoken to throughout our processes have said, 80 percent of the problem that is out there today. Existing threats, we know what they are. We can solve them with existing standards and best practices. How do we get people to implement them? And the key to that is incentives. So some of that—and it is hard to break down whether—what is on the covered line and what is not on the covered line through the legislation process. But in some ways, we need to move forward today trying to get those standards implemented. Whether they are done by covered entities or not by

covered entities, the key is coming up with the right incentives to get people to do that.

Through the Commerce green paper proposal that we are promoting out there, we are trying to emphasize ways that people can do some of these things voluntarily today before the legislation gets enacted and before we would go through this rulemaking process. So we have tried to come up with a number of steps in order to do that, but I do not want to take away from what could be mandated in law.

Senator WHITEHOUSE. My time has expired on this round, anyway, so let me yield to Senator Blumenthal and then to Senator Coons, and we can follow up. We will do a second round. This is a matter of, I think, a lot of interest, and I have a lot of questions remaining.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

You know, in my opening I made reference to the potential threat to our National security from a cyber attack without in any way meaning to predict or even to compare what a cyber attack may mean to the people of the country in making reference to 9/11 or Pearl Harbor, as the soon-to-be Secretary of Defense Leon Panetta did. But it seems to me the American people may have insufficient awareness of the potential for this threat, and I wonder if all three of you, especially Mr. Baker and Mr. Schaffer, because you are in government now, might discuss ways that we can raise that awareness and whether you see there being a threat to the national security from a potential cyber attack.

Mr. SCHAFFER. Thank you, Senator. There is no question that awareness is a critical piece of the puzzle, not just for everyday citizens but for all of the data owners and others who participate in the process. The bill—or the proposal, I apologize, really does have some provisions to enhance a national awareness campaign. We are, of course, already at the Department of Homeland Security working a national campaign to raise that awareness at the consumer level with Stop, Think, and Act in attempts to get consumers to really focus on what they are doing when they are online and whether or not they really ought to be doing that while encouraging them to take advantage of the capabilities that have been brought to all of us in a variety of realms.

If we cannot get consumers to focus and industry to focus and academia to focus, it is much harder to be successful in this realm, and it has to be a shared responsibility across a wide range of actors that we tackle in a variety of different ways, including Cybersecurity Awareness Month and the campaigns that we have ongoing, but we would see that being enhanced through the proposal. I think it is 243(c)(7) where you can find material with respect to the awareness campaign.

Mr. BAKER. Senator, if I could just respond briefly, absolutely yes, this is a threat to the national security. Absolutely without a doubt in my mind. As I mentioned in my opening statement, there are many ways for malicious actors to get into our systems. I articulated three of them: the Zero Day threat, the insider threat, and the supply chain threat—all very big threats, all very difficult to deal with. So that is there.

The important thing for people to understand, I think, is that when a malicious actor gets into a network system, they try to establish frequently a persistent presence in the network. In other words, they want to stay there. Even if we find them in some way and we eradicate them on some system or some subset of systems, they still want to stay there. Once they are in, they want to stay in. And so that is the difficult thing that I think we have to deal with. We have to deal with an environment where it is going to be a degraded cybersecurity environment where we are not going to be 100 percent sure all the time whether the adversary is still there or not.

This is the reality I think we need to face, and I agree that, you know, having hearings such as this, I mean, this is how we educate the American people: statements, you know, the work that this Committee has been doing, that you all do individually. I think that is what we need to—we just need to keep at it to make sure that people have an adequate understanding of the threat.

Mr. SCHWARTZ. Senator, at the Department of Commerce, at NIST, we are helping to run the National Initiative on Cyber Education, or NICE, which is the administration's initiative to coordinate activity across different agencies, including DHS, OPM, DOD, and other major agencies. Each have educational programs, make sure that they are coordinated and work together. That is in the President's budget for 2012, and we hope that it will move forward.

Senator BLUMENTHAL. What about a private right of action that I mentioned earlier. I wonder if each of you could comment.

Mr. BAKER. Well, as you noted, that is not part of the current proposal, and as I said, we are not supposing that this proposal has the answers for everything for all time. And we are happy to work with the Committee and work with you to try to make it better.

There are some things we want to think about, I think, with respect to creating a private cause of action, and I think just generally with respect to the data breach provision—and there have been a number of different suggestions—the one thing to remember is that the companies that have suffered the data breaches are victims of crime. And so we need to acknowledge that and not turn them somehow into criminals through a very heavily regulated type of regime. That is why what we are trying to do is simplify it and make it easier to have a national standard. But the consumers are the ones whose data is now at risk, and we need to make sure that companies that suffer a breach act promptly and act adequately, and we look forward to working with you on what is the right incentive to create to make sure that happens.

Mr. SCHAFFER. Senator, having been a witness to these questions for 15 years from the time that I was with the Justice Department in the Computer Crime and Intellectual Property Section up to today and a practicing lawyer in this space, I think one of the challenges in cyber has always been that there is no real established standard of care and that there is so much variability in the way the networks are put together and in the way that the systems are protected that it becomes very hard to say whether or not someone has lived up to what they should be doing.

One of the things that this proposal does do is it allows industry to participate in developing frameworks and then commit to those

frameworks and develop plans to meet those frameworks in a way that will make it much easier to say, Well, you said you needed to do this in order to secure that network, did you do that? So with a standard of care, I do think it becomes easier, and that is one of the things that you will get through this process.

Mr. SCHWARTZ. One of the things that you heard us all emphasize in the administration's proposal is the role of transparency and the role of disclosure in the proposal on several different aspects. We think that this helps to provide a series of incentives. One of them is the public effects of the disclosure on cybersecurity performance; two, related reputation risk; third is access to government procurement and the related issues to that; and fourth is the perceived litigation risk that comes from knowing how companies are performing, knowing what consumers' information has been taken, et cetera. So that is something that we see as tied into a lot of the transparency pieces in this proposal. We think we can help to build greater incentives around that in the future, including perhaps, as these frameworks build and as this marketplace builds and transparency builds, an insurance market that can help address some of those issues.

Senator BLUMENTHAL. And I understand all of your points and some of your reservations about the private right of action and the need, for example, to define better the standard of care. But I am struck that some of the practices that have led to the breaches most recently are the equivalent of a bank leaving the vault open without any guards at the door: failure to encrypt, failure to take basic safeguards. A bank may be a victim of a bank robbery and claim to be a victim, but if it does not take certain basic steps to safeguard its depositors' money, presumably it should be held accountable. And right now perhaps it can be so by the government, but if you are not going to impose some basic standard and make it enforceable by citizens, I think you are forgoing a basic means of holding these institutions accountable.

My time has expired. You have been very generous, Mr. Chairman. Thank you.

Senator WHITEHOUSE. The Chair recognizes Senator Coons.

Senator COONS. Thank you, Mr. Chairman.

Senator Blumenthal raises some good points I would like to follow up on, another avenue of concern that arises from the same sort of core sets of interest.

The administration's proposal would also provide some criminal and civil immunity protection for entities that share information about cyber threats and assist DHS or other federal entities. And I would just be interested in whether similar protections are currently given to entities that share information with the existing information-sharing and analysis centers. And if not, does the lack of such an immunity or protection deter entities today from reporting relevant information to the authorities that they should? And then I would be interested in your response if there is legitimacy to a concern about good-faith reliance on this immunity and how that good-faith determination would be made. Who would be responsible for making it? Some have raised concerns that this immunity might lead to some recklessness or irresponsibility. And I have a follow-up question on a different subject.

Mr. SCHAFFER. Thank you for the question, Senator. I am going to let Mr. Baker take the good-faith reliance issue, but I will start with what is the problem we are trying to solve here. On any given day, we have entities that are under attack and concerned or they have found something in their own infrastructure that they think is important for the government to know and for a larger community to be able to defend against. That often results in a week-long or days-long process of working with counsel in order to determine and to give comfort to a general counsel somewhere that that information can, in fact, be shared. And in this space, as you know, milliseconds count. Days and weeks are not a good measure of how long it should take to get things done. And the desire is to clear away that uncertainty and give general counsels a comfort level that they can share for this specific purpose subject to the privacy and civil liberties process that would be put in place, which would be extremely robust, but they can share this information expeditiously to protect the larger ecosystem.

And so that is really the problem that we see, days of delay in being able to deploy defensive measures because of concerns around whether or not that can be shared.

Senator COONS. I understand, having been in-house counsel to a company. I think our concern going forward is going to be the civil liberties protections which will be robust, making sure that we, in fact, are able to deliver on that.

Did you have any further comment, Mr. Baker, on the good-faith determination?

Mr. BAKER. Yes, Senator. Under the good-faith provision that you are referring to, I think in terms of who would decide or who would analyze that at the end of the day, I think it would be decided by a court because that is a good-faith defense against a civil action in certain circumstances. And so I think if a provider, somebody who shared information and somebody did not like the fact that they shared information or how much they shared or however it was done, if they were to sue this entity in court, this is how I think the good-faith provision would come into play. And so I think at the end of the day it would be a court, a finder of fact, whether it is a judge or a jury, that would make that kind of determination. So there is protection. That is not something that the government, I think, is going to be deciding on its own. It is going to be before a neutral decisionmaker.

Senator COONS. I understand the value of immunity in terms of speeding up cooperation. I just wanted to flag my concern about how this balance is struck going forward.

A distinct concern of mine or interest of mine, Delaware's National Guard happens to have a cyber warfare unit, cyber warfare squadron that has been stood up, and it happens to take advantage of the unique strengths and abilities of folks who spend much of their career in the private sector working in cybersecurity and then allows them to be double-hatted as folks who are connected to our Nation's national security apparatus.

Do you see a role for the National Guard going forward as something that could be a useful bridge between cyber law enforcement needs and cyber defense needs and tap into some of the growing strength in terms of the civilian population in the private sector's

resources and training, first and second? And then how do you think we are doing at standing up and training a sufficient cadre of qualified cybersecurity professionals in the private sector to augment the execution and delivery on the sorts of policies you are expecting the private sector to be able to act on in this proposed set of administrative policies?

Let the record reflect Mr. Schwartz declined to comment.

[Laughter.]

Mr. SCHAFFER. Senator, thank you. Certainly, as we have said, there is a role for everyone to play in this space. There are needs for all of us to participate in buying down risk and making sure that we are addressing cybersecurity across a very large domain.

I do think that there are opportunities both in this proposal where we would like to do an exchange to allow government and industry to be able to exchange some personnel so that we learn how others do this. There is some tremendous value for those who have gone from government into industry and from industry into government in terms of having us understand the challenges on both sides of the fence, and this proposal includes some of that. It also makes it easier for us to do some hiring. As was pointed out, there are initiatives from an education perspective to try to get to a higher level of capability across the board for cybersecurity, and there are several initiatives that currently attempt to do that by working with the universities and even with the elementary schools to start people thinking about cybersecurity as a career much earlier in the process.

So there is a range of things that I do think need to be done. We very much share the notion that public awareness is going to be a critical part of this process, and the need to bring as many people into the fold as possible is certainly part of what we are trying to get to.

Senator COONS. Thank you.

Mr. Baker.

Mr. BAKER. Senator, just briefly, to echo what Mr. Schaffer just said, I think we really do need to adopt a whole-of-government approach to this problem. We need to look at all the resources that we have, and I think it is sometimes useful—analogies are always difficult, but if you think about how we have tried to deal with the threat from terrorism and how we have utilized all parts of the U.S. Government—from the transportation sector to the FBI, to the intelligence community, to the military—we have made sure that we have used all of our resources. And I think that is the kind of national effort that we need when dealing with the threat that we are facing today because I think it is that big and it is that multifaceted, so we need to make sure that we are bringing all of our resources to bear.

So I think your idea is worth exploring. We will have to give some thought to it. I do not know off the top of my head exactly how that would work, but, you know, everybody who has a skill and ability in this area needs to be utilized to the full extent possible.

Senator COONS. Well, thank you, Mr. Baker.

Thank you, Chairman, continuing to be so effectively engaged in this difficult issue that is important for our National security.

Senator WHITEHOUSE. Thank you, Senator.

Let me go back to where we left off, and I think what I will do is I will make this a question for the record so we just do not bog down this hearing getting way into this. But what I am interested in is what elements of the ISP system are expected by the administration to qualify as critical infrastructure under its proposal for requiring approval of critical infrastructure protection. And this is potentially a related question, depending how the answers come down, but the related question is: Where in the administration's proposal is the ISP customer relationship regulated with respect to giving customers notice that they are the unwitting and unwilling bearers of viruses, malware, and other threats?

[The information referred to appears as a submission for the record.]

Senator WHITEHOUSE. The other area that I wanted to touch on is with respect to reporting. Basically when is a hack not a breach? There is considerable emphasis in the administration's proposal on data breaches, particularly ones that cause the disclosure of significant amounts of public information. But the threats in various areas are not just the breach of privacy and the loss of public information. They are the loss of intellectual property by a company. They are the insertion of malware into critical operating systems, things like that. Where do you propose that things other than data breach be reported? And is that an area that is open to be worked on? Should publicly traded entities be more clear in their SEC filings about the risk that they face from cybersecurity? Clearly they are spending a lot of money on protection, but are they reporting what they are doing? Is there daylight into that? Are the key commissions—the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the FAA—obliged to assemble data about the risks that the industries that they regulate are at risk of suffering? And probably you would want to de-identify the information so that you are not creating competitive advantage and disadvantage, but at least you would want the public to know—back to the conversation about public awareness, you would want the public to know that a federal regulator has stepped out and said, oh, by the way, here are the major risks to the electric grid, here are the major risks to the air traffic safety, here are the major risks to nuclear facilities.

Now, some of it is going to be classified, but I think it is important that we kind of bring all of that up, because my concern is that you can have national awareness campaigns until you are blue in the face, but if the actual attacks are classified when they had dot.gov and dot.mil and kept proprietary by business so as not to alarm customers and regulators and consumers and competitors—or I guess encourage competitors—when it is dot.org and dot.com, then, you know, you have a real information deficit and the American public is being denied a lot of information that they should have and that they could perfectly well have if it were de-identified so that you were not targeting a particular bank or a particular utility, but just letting people know this is what happened today, this is what happened today. And I do not see how you can inform the public adequately without the underlying information becoming

more clear, and I do not know how you do that in this piece of legislation.

Mr. Schaffer.

Mr. SCHAFFER. Yes, Senator, thank you. There is in the proposal—and there are many notice provisions. There is a proposal that would require those who are in critical infrastructure to share promptly, report to the Secretary of Homeland Security any significant cybersecurity incident. So within that class that would fall into the critical infrastructure, you would have a notice requirement not dependent upon a particular PII, or personally identifiable information, having been accessed but just——

Senator WHITEHOUSE. And that is in that same critical infrastructure category that my first question was about, the one that you have taken for the record.

Mr. SCHAFFER. It is.

Senator WHITEHOUSE. Okay. Outside of that. So you have got critical infrastructure, and you have got these big data breaches. What else?

Mr. SCHAFFER. Outside of critical infrastructure this particular provision would not apply, but I do think that some of what has been happening in the last several months with breaches is instructive in that the structure that we have now, the National Cyber Incident Response Plan, and the ability to work through the National Cybersecurity and Communications Integration Center at DHS, which has representatives from industry who literally sit on the watch floor with DHS, with law enforcement authorities, with authorities from other parts of government, gives us the ability to share that information much more effectively and efficiently. And, indeed, if you look at some of the recent incidents, within an hour or two of an announcement being made, we will have assembled a cast of players who have an interest in the issue and will have gotten them engaged in discussing mitigation strategies.

In some instances we are able to push out information to specific sectors even before there is a public announcement by the entity that is impacted, and so I think that construct is starting to work in the way that we had always envisioned it would, and that does allow us to get information out much more aggressively.

Senator WHITEHOUSE. About a specific incident to people interested in that specific incident as opposed to more across the board.

Mr. SCHAFFER. Yes, certainly to government, CIOs, and CISOs in very short order, and to interested parties in the private sector. The whole construct that we have now is to try to get out through the Information Security Analysis Centers, get information out to an entire sector or segment of the economy as quickly as possible that information which can be most useful for them in deploying defensive measures.

Senator WHITEHOUSE. Against a particular attack. I meant more generally about just having there be more awareness of the extent of the attacks that we are under. I think that—I will find that. Here we go. Symantec says that it recorded over three billion malware attacks in 2010, and that is nearly a 100 percent increase. That is billion with a B. There is a huge disjunction between what is really happening out there and what people know, and just letting people who might be compromised in a similar way by a par-

ticular attack now is important and is valid, and I am glad you are doing it. But it is a different thing than raising the general level of public consciousness about all of this so that people are more inclined to take protections, more inclined to buy the commercial off-the-shelf technology, more inclined to do the various steps that will protect them.

Mr. BAKER. Senator, on your question just very briefly.

Senator WHITEHOUSE. Yes, Mr. Baker.

Mr. BAKER. With respect to your reference to the SEC, I just would note that some companies have begun to make reports about intrusions that they have suffered in their filings with the SEC, so——

Senator WHITEHOUSE. And Senator Rockefeller and I and others have sent a letter to the SEC asking that they beef this up, and they are looking at it right now and will get back to us later.

I am going to recognize Senator Klobuchar in a moment, but let me ask one more question since we are sort of on this subject.

It seems to me that one of the things that we can do that would be very helpful would be to encourage conversation about threats. You talked about immunity and making sure that, you know, the conversation between DHS and affected businesses is safe conversation. But we have the defense industrial base out there talking to one another about cyber threats. You have the ISACs in different industries out there beginning to talk to each other about various cyber threats. I am hearing from a number of folks that those are processes that are both, A, very useful and, B, not anywhere near as robust as they could be because of a variety of hesitations from the participants about their participation in that internal industry group, that they might lose protected status of information, proprietary status or privilege, that they might face an antitrust challenge for what they are talking about in there. And we are sort of operating in a legally uncertain zone in doing this.

The proposal of the administration is that when it is business to DHS, that is a protected discussion. But there is no protection for the B2B discussion within these industrial organizations or groups that are already set up to try to do this.

Are those effective? Should their work be enhanced? And what do you think are the best ways to enhance their work in ways that do not require government intervention? That is just basically the industry circling its wagons against common threats and trading information and engaging in common defense, like the old prairie schooners of yore.

Mr. BAKER. Just very briefly, and then I will turn it over to Mr. Schaffer. We have spent a lot of time thinking about that. You are exactly right. That is an important issue. We recognize that. We have looked at it closely. We have looked at a variety of different ways to do this.

There are some tricky legal issues in there. As you mentioned, the antitrust concern I think is one that is of particular note, and so we have to focus on that. But I think, you know, we are open to working on that issue. We recognize its importance, and you are exactly right. We need to figure out a better way to enhance that sharing and balance all the different factors that you mentioned that have to be balanced appropriately.

Senator WHITEHOUSE. And recognize that for a lot of the participants in these things, it is a game in which it is to their great advantage to be the free rider who does as little as possible and allows their industry colleagues to carry as much of the load as possible, and when everybody is looking at it that way, you do not get an optimal result. So there is kind of an economics and motivation problem built into it as well.

Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Senator Whitehouse. Thanks for chairing this hearing, and thank you to our witnesses. I am sorry I was late. We have the Commerce hearing for the new nominated Commerce Secretary, which also has some role in this cyber area, and I am actually currently working on a bill with Senator Hatch from this Committee on cloud computing, and I think updating some of our laws in light of the technological advances surrounding this innovative business model is very important. I think it has the potential, cloud computing does, to alleviate some of the concerns in the cybersecurity field by introducing economies of scale and making sophisticated protection available to all cloud users. But it also raises some unique diplomatic issues because data is being stored in multiple countries.

Can you talk about the issues of international jurisdiction faced by your agencies when investigating cyber crime involving cloud computing? Does anyone have any—Mr. Baker?

Mr. BAKER. I will start Senator. Thank you. Yes, the number of different issues—and I have testified before the Committee on some of the ECPA issues that are at play with respect to cloud computing, so we recognize the importance of it. The administration wants to do everything it can to support the development of cloud computing industries.

It does raise a number of security issues, as you just highlighted, and I think that the thing about this data and the thing to remember about the various structures that we have is that the Internet is a physical thing, and it exists in different places. And the data, as you mentioned, is stored in different places, and so it raises these different jurisdictional issues. But one of the things we have focused on, in particular, for example, at the FBI, is working with our international partners on these investigations, because the cyber criminals in particular move around to lots of different places and try to obscure where it is that they are coming from and who they are attacking and so on.

And so the international issues are only going to get greater, as you highlight, but we at least, at the FBI and the Department of Justice, have focused extensively on trying to make our international cooperation better than it has been.

Senator KLOBUCHAR. Do you think better international agreements on the rules relating to data shortage against bad actors would help you with fighting cyber crime?

Mr. BAKER. I think depending on how they were structured, I think they could, certainly, yes.

Senator KLOBUCHAR. You would not want a bad international——

Mr. BAKER. Right. Exactly. Right. Exactly.

Senator KLOBUCHAR. Okay. Good.

Mr. SCHWARTZ. Senator, we completely agree with you on the point about the cloud and economies of scale and how it could end up helping security, particularly with small companies and small agencies that themselves have to invest a lot to protect security today.

One proposal that we do have in the administration proposal is a piece on promoting cloud services tied to ensuring that—preventing States from requiring companies to build the data centers within a particular State, except where that is expressly authorized by federal law. We think that that will help for companies to feel better that they can invest in the cloud and help create international norms around the cloud. We have seen some countries already where the provinces or states in those countries have passed laws saying that you must locate cloud storage within our jurisdiction, particularly to address the kinds of concerns that you are talking about. We do not think that is the right way to go to address those concerns. We think that we need to let the cloud, the marketplace for the cloud, flourish and then have enforcement happen through the channels that you are discussing with Mr. Baker.

Senator KLOBUCHAR. Okay, very good.

What tools does the administration's proposed cyber legislation give the Department of Justice to more effectively investigate and prosecute the offenders both domestically and internationally?

Mr. BAKER. Well, there are a number of different provisions that would assist us, so the data breach proposal is one that would give us a heightened awareness of what is happening, more prompt notification of what is happening, and that would certainly enable us through the various reporting requirements that are part of that proposal in terms of notifying the FBI, that would certainly enhance our situational awareness, as we say, about what is going on.

The various amendments that we have proposed with respect to the Computer Fraud and Abuse Act and other federal statutes, such as the RICO statute, to make certain violations of——

Senator KLOBUCHAR. Could you elaborate on that—I used to be a prosecutor—how amending the RICO statute would be helpful?

Mr. BAKER. Sure. As I mentioned in reference to the other questions, many of the crimes that we are facing and the criminals that we are facing are organized criminals, and so we think it is totally appropriate that we use a tool that is intended to deal with organized crime, the RICO statute, to counter some of those activities. And so it seems to make sense to us. It is pretty straightforward, frankly, and it is a powerful tool. We know people have concerns about it. We want to use it responsibly. We think we have in place the adequate administrative controls inside the Department to use it responsibly, but we think it is something that could benefit us significantly.

Enhanced penalties for certain efforts or crimes involving damage to critical infrastructure computers we think would help us also. Also bringing some clarity to the penalty provisions that are part of the Computer Fraud and Abuse Act we think would also help us and enable—or enhance our deterrence in that area. It is difficult. In order to—I think as Senator Whitehouse was saying—in order to investigate and prosecute the crime, you have to find

out about it. You have to have the resources to be able to investigate it and so on. We know that. That is all part of the piece. But clarifying some of the penalty provisions, for example, and these other things I mentioned-——

Senator KLOBUCHAR. And could you just elaborate on that? I have been working in the area of some of the streaming issues to try to come up with a way with a number of the other Senators to acknowledge that if someone is standing on a street corner and sells DVDs that are over $2,500 that we already know is a felony, and right now if you do it, if you have a business and you are illegally selling anything—movies, books, music—and you do it maybe $1 million and you are profiting—you have to profit from it under our bill—it is still a misdemeanor. And so we are trying to fix that without, you know, hurting anyone's rights or teenagers that are simply trying to share some information. So we have a lot of issues with it. It reminds me a little of this as you try to look at what the penalties are without doing anything that would hurt innocent people in how you are trying to do it.

So could you talk about that with the cybersecurity and the penalty issue?

Mr. BAKER. Certainly. To your point generally, we definitely understand concerns that folks have expressed with respect to some parts of the *Computer Fraud and Abuse Act*. We understand that. We get that. We are trying to use it appropriately under the circumstances in making prosecution decisions in light of the various guidelines, and in full knowledge that we have to justify what we are doing both to the Congress and to the courts that we prosecute these cases in front of.

With respect to the penalties, the *Computer Fraud and Abuse Act* statute has got a lot of different features to it. There are a lot of things that it tries to prohibit, and it tries to do it in a variety of different ways, and it tries to look at what the intent is, what the amount of damage that is involved is, what the activities are that are at issue. It is not just a hacking statute. It is more than that. But it is a variety of different crimes that have to do with computers that we think enable us to prosecute things and crimes that the country wants us to prosecute.

Senator KLOBUCHAR. I think it is hard sometimes for people to understand that if someone used a crowbar and broke in and stole all of your DVDs, that is clearly a felony. And then they are stealing things off the Internet, it is also a bad crime, whether it is your personal identification or someone else's property. I just think it is a challenge of our day to make our laws as sophisticated as the people who are breaking them without doing it in a way that brings in innocent people. But I do not think that should make us turn away. I think we have a challenge of making the laws work right, but we are up for that challenge; otherwise, we are just basically conceding this to crooks on the Internet. We have to find a way to do this right, so I appreciate it. Thank you.

Senator WHITEHOUSE. Thank you, Senator Klobuchar.

Mr. Schaffer, you said a little while ago that milliseconds count when you are doing this defense. You cannot wait hours or days for lawyers to do their thing. It is also true that sometimes milliseconds are too late, that if you have not pre-positioned certain de-

fenses, you are out of the game, or you are in a different game in a much worse position than you would have been otherwise.

We have to be careful what we say because this is a public hearing, but clearly there are some capabilities that the U.S. Government has that would be useful if they were allowed to defend particularly critical infrastructure. Is there any vehicle for the U.S. Government to deploy classified measures to protect critical infrastructure in this bill without having to get the request and the approval and the cognizance of the owner of the critical infrastructure? Is it not the case that you would basically have to read into any classified program that was used the operator of the critical infrastructure or not use the program to defend the critical infrastructure? I think we need to bridge that gap, and I do not see how the bill does that.

Mr. SCHAFFER. Senator, there is not a provision in the current proposal that would provide for that. We do have capability that is coming along with respect to Federal Government critical infrastructure, that which is owned by departments and agencies or managed by departments and agencies, through the intrusion prevention programs that we have intrusion detection widely deployed now for federal departments and agencies. We are in the process of building out intrusion—we have intrusion detection, excuse me. We are working toward intrusion prevention, and——

Senator WHITEHOUSE. And you have the advantage in all of that where it is the Federal Government involved that you have by definition single-party consent to the methods that are used to protect that infrastructure. Once you get outside of the government and you now have critical American infrastructure that is privately owned, it is very hard to deal with that consent issue, particularly if it is a classified program. In that regard, I would be interested in your thoughts on what the former head of NSA and others have suggested about having a secure domain into which critical infrastructure could be located that would, by its very existence, be a signal to anybody going there that the very best capabilities of the U.S. Government are being deployed in this area in the same way that people going to dot.gov and dot.mil are signaled in that exact way right now. It seems to me that we have critical infrastructure that is far more important than some of the things that are protected by dot.gov and dot.mil. Not everything but some. And yet the standard of what we do to protect dot.gov and dot.mil is much higher than even critical infrastructure in the open Internet.

The second thing that that would do is it would also tell you where that was not going on, and it would provide the public assurance that they are not having their communications scanned or screened or swept in any way by the government if they are just on eBay or if they are in a chat room or if they want to do the sort of ordinary noncritical commerce and information exchange that the Internet supports.

What are your thoughts about that idea?

Mr. BAKER. I will just add the legal question for a minute and then turn it over to my colleagues for more of the operational things.

Having said that, let me just say at the outset the sharing of classified information in many ways is more of an operational issue

as opposed to a legal issue, I think, if the government is sharing with the private sector.

Senator WHITEHOUSE. Right.

Mr. BAKER. That has to do with the confidence that we have in sharing the information that it is not going to get out and be disclosed in some way. But having said that, in terms of the type of secure environment that you are talking about, you would have to do the type of legal analysis that would look at all the various surveillance statutes that would apply in this area, because they apply not only to the government, they apply to the private sector as well. You have to think about and look at the extent to which the government, in fact, is doing this through some type of agency relationship with the private sector, depending upon the nature and scope of the relationship that we have with these various entities and how that all evolves, and that——

Senator WHITEHOUSE. Depending on the agency relationship, it could easily become a government act.

Mr. BAKER. Exactly.

Senator WHITEHOUSE. Giving rise to all of the Fourth Amendment concerns that pertain here.

Mr. BAKER. That is exactly right. That is exactly where I was going. So we have to think about all those things. Can you get through that analysis? Yes, you——

Senator WHITEHOUSE. But a domain clears that issue, does it not, by making people aware so that there is consent before you enter it?

Mr. BAKER. That is a tricky question, I think. You may not need consent in every instance in this type of situation if there was some type of special need for the government with respect to the cybersecurity activity that is at play. Whether the special needs doctrine applies and whether we meet the requirements of it is going to be a fact-specific inquiry, I think. But it is something that is worth looking at, and we understand these ideas. We have heard about them, obviously, and we are working on developing these types of ideas. And so it is something that we definitely want to look at.

Senator WHITEHOUSE. The fact of the matter, it seems, is that unless you are willing to disclose certain highly classified programs that are kept away from a lot of people we trust, even in the military, even in the government, because of their—you know, classifying is what is necessary to keep them secure. Unless we are willing to share those with fairly large sectors of the private industry, because it is hard to pick winners and losers and say, Okay, we are going to protect you because we trust you, but this other utility that has a CIO who comes from Estonia and we are not sure about their cousin and so we are not—you know, I am making all that up, but you can imagine the complications that you get into when you start making those choices.

I think the bottom line is that we have—there are resources that could protect private sector critical infrastructure but will not without declassification to a degree or without a risk of declassification that we may not be willing to face. And it seems to me we solve that problem if we make it more clear and overt, what we are doing. And there is no real magic to it. You just say, okay, look,

if you want to go and look at these electric grid things, you have got to be aware that the government is going to be keeping an eye on what goes in and out of there in order to protect the electric grid. I do not think people mind that. And then they know it is not somewhere else as well.

Mr. Schaffer.

Mr. SCHAFFER. Senator, for reasons that you alluded to at the beginning of the question, I think we would like to come and talk to you about this further, perhaps in another forum where we can go into a more fulsome discussion about all of the parameters. But suffice it to say there is, as you point out, quite a lot of complexity both from a legal perspective, a technical perspective, and other perspectives——

Senator WHITEHOUSE. A security perspective.

Mr. SCHAFFER [CONTINUING] In terms of how you would address this issue, and so I would suggest that perhaps we make arrangements to give you a more full briefing at another time.

Senator WHITEHOUSE. That is fine. You will agree with me that there is an issue that is worth pursuing, though.

Mr. SCHAFFER. Certainly worth having the conversation.

Mr. SCHWARTZ. I will say that it is an issue that is under great discussion among the interagency groups that work on these issues. We are continuing a discussion about that, and we look forward to working with you on it.

Senator WHITEHOUSE. I have to assume that the interagency process is sort of an ongoing thing and that there remain discussions going on within the administration on these subjects. That would be only logical, and I assume that that is the case. Correct?

Mr. SCHWARTZ. Many, many, many meetings.

Senator WHITEHOUSE. Good. Another topic I wanted to raise is the issue of prosecution and investigative resources. I will direct this more to you, Mr. Baker, since I think the Department of Justice is going to be the primary actor here. This is a new area. It is a growing area. It is an area of, as each of you have indicated in your testimony, intense concern both from an economic, from a criminal, and from a national security perspective. In the past, when we have had grave concerns, whether it was things like alcohol, tobacco, firearms, and munitions, entire agencies have been stood up to deal with it. When it was narcotics, the entire Drug Enforcement Administration was stood up to deal with it.

By contrast, what we have addressing the cyber crime and cybersecurity threat is considerably smaller, which does not necessarily by itself mean that you have got to blow it up, but these are also very, very significant cases in terms of resource intensiveness. You are dealing with highly specialized electronic information about how the Internet works. You are dealing with players who are located in foreign countries. You have immense complexity trying to investigate across foreign borders to find these folks and to work through the different treaties that permit all of that. You have not only the need to make criminal prosecutions but very often to build civil cases in order to shut off certain things, as you all did so well in the Coreflood Botnet and as Microsoft did in the Waledac botnet.

This is a lot tougher than your ordinary drug case. This is a lot tougher even than your ordinary RICO case. This is international RICO-type investigations with a huge technical overlay to them. So with all of that, what do we do to resource up enough so that we can address these cases as aggressively as many of us believe we should? Are you satisfied that the existing resources will do the trick, or do we need to think about scaling up to meet this threat?

Mr. BAKER. Thank you, Senator. I think from the Justice Department's perspective, obviously we can always use more resources in this kind of area. We are trying to—we know there are limited resources available, and so we are trying to use them very judiciously and effectively and not just chasing everything that sort of pops on the radar screen. We are trying to be thoughtful about this, and the NCIJTF, National Cyber Investigative Joint Task Force, is focused very much on trying to get the most bang for the buck, if you will, on the resources that we have available.

I will say—and I would imagine that my colleagues would echo this—you cannot just grow good cyber investigators and prosecutors overnight, and so we need to have a long-term view of this and grow our resources properly and effectively because, as you mentioned, we need experts, we need people who really know how to work these cases. This is not a problem you can just throw bodies at and just pull people in and have them start working these cyber cases.

Senator WHITEHOUSE. But that said, you do believe that, as time goes forward, this is going to be an increasing threat for the country, an increasing responsibility for law enforcement, and we are going to need increasing resources in order to meet that threat.

Mr. BAKER. Absolutely, and I think that the projections that I have seen in terms of the budgets going forward have a steady increase, so far that I have seen at least, in terms of the folks that we have to devote to this, not only the investigators but the prosecutors that can bring these cases to court as well, who understand what is happening and who can come up with the kinds of ideas, as you mentioned, that the prosecutors and investigators came up with with respect to the Coreflood activity.

Senator WHITEHOUSE. Mr. Schaffer, did you want to comment?

Mr. SCHAFFER. Yes, Senator, thank you. I think that what you have seen in DHS' space is that we indeed have been growing dramatically, tripling the size of our National Cybersecurity Division in 2009 in terms of federal employees, doubling again in 2010, or nearly doubling, and continuing to grow and projected to grow in the 2012 budget as well. So we are on a trajectory to bring additional resources on, as pointed out in the proposal. There are some challenges in getting access to the very best people, which is what we want, but we are moving forward to grow the program. And, of course, cybersecurity as an issue area has been elevated to one of the top five mission areas for DHS in the Quadrennial Homeland Security Review.

So we certainly have tremendous focus on this at DHS. I think that is echoed throughout the administration. All of the departments and agencies recognize this as a very significant area and an area where attention is going to have to be paid for an extended period of time.

Senator WHITEHOUSE. The last topic I would just like to ask each of you on—I know I have kept you a long time, and I appreciate it—is the question about the supply chain. On the one hand, we have a very well-developed and very efficient international, global supply chain for electronics in particular. And by and large, as we have seen from the development of these products, it has served American consumers and people around the world very well. And the products that have been launched and the services that have been launched, I think, have served humankind very well. The Arab Spring is largely the product of that technology.

All that said, it is increasingly a threat to the country that foreign governments working with foreign suppliers could go about planting into our supply chain not just defective products or counterfeit products of the nature that I have just done a military counterfeit bill on, but products that actually allowed for infiltration and access into the other computer or the system that it is connected to. And you do not want to shut down the very vibrant global supply chain that supports the industry. On the other hand, we have got to protect against that kind of a risk, particularly with the United States as the primary target, both as a national security target around the country and around the world and as the biggest user and the economy that is most dependent on the Internet.

What is your advice with respect to supply chain security? And where does this bill begin us on that discussion?

Mr. Schaffer.

Mr. SCHAFFER. Mr. Chairman, I think that the supply chain issue is one of the most challenging and complex issues in cybersecurity today. Because the supply chain is so robust, because U.S. suppliers and foreign suppliers are very much intertwined, both in terms of products that U.S. companies are putting in the market, that U.S. companies are developing in other parts of the world, that foreign companies are using U.S. equipment in their equipment, it becomes very challenging.

And so the administration is very aware that there are challenges here and is focused on that. There is an administration task force that is led by DHS and the Department of Defense to think about those issues and to try to develop methodologies to mitigate risks associated with supply chain and to identify long-term solutions that can maintain U.S. industry in a robust way and also have a level playing field for products and services as we go forward.

So that is a challenge that I think we will be addressing and thinking about for some time, and I do not know that we have——

Senator WHITEHOUSE. So it is nothing specific to this legislation. We will just have to keep working on that one.

Mr. SCHWARTZ. Mr. Chairman, we look forward to working with you on this extremely important issue. One thing that I think is worth noting as well—I think Mr. Schaffer did a great job at laying out the basic outline of the kind of work that is going into this in an interagency context, but one thing that is important in all these issues but it comes out more clearly in supply chain, is this idea that whatever we put on companies through trade, we also have to be willing to accept internationally. We have to think about this in a global way, that our companies in the U.S. have to work inter-

nationally as well. We have to come up with policies that work internationally both for imports and exports. What will be expected of companies that are importing we have to also expect for the companies that are exporting may have to live by those same rules, and we should expect that to be the case.

So we think that we can come up with global solutions in this space and in the cybersecurity realm in general, and that is one of our targets as well.

Senator WHITEHOUSE. Very good. Well, let me thank you all. You have taken a lot of time this afternoon. I appreciate it.

I want to close by referencing some of the private sector conclusions that have been drawn in this area. On the Senate floor, I have already spoken about the McAfee Night Dragon report, but I just want to quote it here.

"In 2010," McAfee says, "we entered a new decade in the world of cybersecurity. . . . This decade is setting up to be the exponential jumping-off point. The adversaries are rapidly leveraging productized malware toolkits that let them develop more malware than in all prior years combined, and they have matured from the prior decade to release the most insidious and persistent cyberthreats ever known."

Focusing on the Night Dragon attacks, it says, they worked "by methodical and progressive intrusions into the targeted infrastructure. . . . While Night Dragon attacks focused specifically on the energy sector, the tools and techniques of this kind can be highly successful when targeting any industry. Our experience has shown that many other industries are currently vulnerable and are under continuous and persistent cyberespionage attacks of this type." That is McAfee.

Symantec, very similar, the overall conclusion: "several significant events in 2010 suggest that advanced and persistent cyberspace threats have leapt to a new evolutionary stage. . . . This evolutionary leap leaves public-sector cyberspace defenders scrambling to address technological, operational, and procedural gaps in the wake of their adversary's rapid maturation. . . . The defense of critical operations requires cybersecurity personnel to assume that netwoked systems can be compromised."

And they describe an operation called Operation Aurora: "the sheer scope of Operation Aurora differentiates it from previous attacks of this nature. . . . The operational scope implies that the threat actors were highly organized and their goals extremely focused. It also reflects [that]. . .it is no longer a question of whether or not adversaries will use cyberspace to assist espionage—they will—and it must be part of the basic assumptions made by security practitioners, whether practicing in the public or private sector."

It is compelling when two of the largest and most renowned security providers say virtually the same thing in reports about the exponential jumping-off nature of the threat that we face, and I appreciate immensely the work that you all are doing to try to protect us from that, to try to keep up with the threat as it metamorphoses. And I think that in the areas that we have discussed today, the areas of broader reporting so that the public is more aware of these concerns, in the area of the ISP responsibilities toward their

consumers to let them know about when they are unwitting and unwilling bearers of malware and viruses, including these particularly threatening new ones, potentially, in the business-to-business relationship, the ISACs, the DIB, and the other areas where we want to encourage those communications, with respect to advance positioning of some of our most critical defense around our critical infrastructure, with respect to adequately resourcing the law enforcement side of this, and with respect to protecting particularly our military, defense, and critical infrastructure supply chain, we have quite a lot of work to do.

I look forward to working with all of you as the administration's proposal goes forward and is amended and amplified through the legislative process. And thank you for the work that you have done on behalf of our country.

The hearing will remain open for another week for any testimony that may come in. I would be delighted to get the QFR responses from you within a couple of weeks, if that is possible. And there is a statement from the Financial Services Roundtable that we will put into the record of this proceeding as well as the complete statement of Representative Langevin of Rhode Island.

[The statement appears as a submission for the record.]

Senator WHITEHOUSE. And I will add also a report from the Center for Democracy and Technology entitled "Cybersecurity: Evaluating the Administration's Proposals," dated June 21, 2011.

[The report appears as a submission for the record.]

Senator WHITEHOUSE. That completes the record of the proceeding. Again, I thank the witnesses, and we will be adjourned.

[Whereupon, at 4:26 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

On

"Cybersecurity: Evaluating the Administration's Proposals"

Tuesday, June 21, 2011
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

The Honorable Jim Langevin
United States Congressman
State of Rhode Island

Panel II

James A. Baker
Associate Deputy Attorney General
U.S. Department of Justice
Washington, DC

Greg Schaffer
Acting Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security
Washington, DC

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
Washington, DC

PREPARED STATEMENT OF CHAIRMAN PATRICK LEAHY

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism
Hearing on "'Cybersecurity: Evaluating the Administration's Proposals"
June 21, 2011

I commend Senator Whitehouse for holding this timely hearing about the administration's cybersecurity proposals. I also congratulate him for his dedicated work as the Chairman of the Subcommittee on Crime and Terrorism.

Developing a comprehensive strategy for cybersecurity is one of the most pressing challenges facing our Nation today. In the digital age, we are witnessing truly fantastic advances in technology. But, with the explosion of new technologies, such as social networking sites, smartphones, and mobile applications, we also face threats to privacy and to cybersecurity like at no other time in our history.

In just the last few weeks, we have witnessed major data breaches at Sony, Epsilon, RSA, the International Monetary Fund, and Lockheed Martin -- just to name a few. Recently, Google announced that the Gmail accounts of hundreds of its users, including senior U.S. Government officials, have been hacked in an apparent state-sponsored cyber-attack. Our Government computer networks have also not been spared -- as evidenced by the recent hacking incidents involving the Senate and Central Intelligence Agency websites.

We cannot afford to ignore these threats, or their impact on our privacy and security. That is why I have made protecting Americans' privacy and security in cyberspace a top priority for the Judiciary Committee.

As Chairman of the Judiciary Committee, I am working closely with the Obama administration and others in Congress to develop a comprehensive national strategy for cybersecurity. Earlier this month, I reintroduced my Personal Data Privacy and Security Act - a comprehensive data privacy bill which would establish a national standard for data breach notification and require

that companies safeguard our sensitive personal information. Many of the sound privacy principles in my bill were included by the administration in its cybersecurity proposal.

The privacy protections in that bill are long overdue. In fact, I have introduced the legislation four times and each time I have done so, the threats to data privacy have been greater than the time before. I hope the fourth time is the charm.

In the coming weeks, I will include this bill on the Committee's business agenda, so that we can consider and hopefully promptly report the legislation again. In the past, the work to pass this bill has always been a strong bipartisan effort. I hope that it will be so again this time.

I am pleased that representatives from the Departments of Justice, Commerce and Homeland Security are here to share their views on how best to protect cybersecurity. I look forward to learning more about these proposals.

We simply cannot wait to act on comprehensive cybersecurity legislation. But, we must proceed in a way that is respectful of our privacy rights and civil liberties.

We must also work together -- across party lines and ideology -- to build a secure future in cyberspace. This is not a Democratic issue, nor a Republican issue -- it is a national issue that impacts all of us. That is why I hope that all Members of the Committee will bring a bipartisan spirit to our work to strengthen our Nation's cybersecurity.

Again, I commend Senator Whitehouse for holding this important hearing. I look forward to a good discussion.

#####

PREPARED STATEMENT OF HON. JAMES R. LANGEVIN, A CONGRESSMAN FROM THE STATE OF RHODE ISLAND

Statement of Rep. James R. Langevin
Ranking Member on House Armed Services Subcommittee on
Emerging Threats and Capabilities

Hearing Before the Senate Committee on Judiciary
Subcommittee on Crime and Terrorism

June 21, 2011

I would like to thank Chairman Whitehouse and Ranking Member Kyl for inviting me to testify before the Judiciary Subcommittee on Crime and Terrorism on one of the most critical national security challenges facing our country today, and the Administration's proposal to address this threat. Cyber incidents have grabbed headlines in recent months, with our top companies seeing intrusions and loss of data, and our constituents are beginning to realize that the internet is a highly contested space where personal information is never truly secure. What is not receiving much attention, however, is the fact that these incidents come from highly diverse actors, go after very different targets, and result in a broad range of consequences. The incidents range from what appears to be a new form of protest, referred to as "hacktivism," against soft targets such as the public websites of companies or government agencies, all the way to highly advanced nation-state actors involved in persistent and stealthy espionage of state secrets. The common thread is that the threats all exploit our strong reliance on the internet for social communication, business, and national defense, and will only increase as that reliance grows.

Let me first address an issue I believe Congress can easily support, once it receives the attention it deserves, and that is the crisis we are facing in highly skilled cybersecurity professionals. Our nation is a leader in internet security technology both in the private and federal sector, but we do not have enough highly trained individuals to match our growing needs. Nor do we have a strong pipeline for bringing talented individuals with an interest in computer security into the workforce. In 2008, Jim Gosler, the founder of the CIA's Clandestine Technology Office, estimated the U.S. only had 1000 security specialists with the advanced skills necessary to operate at a high level in cyberspace, while the number needed is closer to 20,000 or 30,000. However, since we have learned of this deficit, our workforce has stagnated, while the threat continues to multiply.

In Rhode Island, we are working to educate our future workforce for 21st century cybersecurity jobs. Earlier this year, we launched a pilot program with the Center for Internet Security to engage high school students in cybersecurity skills through competition. We had nearly 100 participants and local businesses offered internships to several of our winners. The University of Rhode Island also recently hosted a major symposium where federal, business, and academic leaders joined together to identify new areas for cyber research and development. As a result of this conference, we are building a statewide Cyber Center of Excellence that will work to grow the cyber workforce in Rhode Island, while meeting an increasing need for a strong public-private relationship in cyberspace.

As we prepare our workforce to meet these challenges, we must bring our laws and policies in line with the realities of today's internet, and I appreciate the Administration's proposals to move our nation in this direction. Since the first malware appeared in the early days of the internet, software has been created to offer a technical solution to make our systems and data more secure. Year after year this software has grown more complex, powerful, and expensive, while malicious code remains cheap and often easily procured. An analysis by the Department of Defense shows that since the late 1980's, the lines of code in security software have grown exponentially, while the lines of code in an average piece of malware have remained nearly constant. Unfortunately, this pattern shows that our security measures are divergent from the threat and that technical solutions alone are not enough to secure our valuable systems.

There are three policy areas under this Subcommittee's jurisdiction that I would particularly like to address: the White House's recommended penalties for cyber crime against critical infrastructure and racketeering; national data breach standards; and voluntary information sharing. While I understand that the Administration's proposal was intended to be taken as a whole product, I believe these three elements are especially important. As I discussed earlier, the foundations of trust and known identity on which the internet was built have enabled criminals to take advantage of those using the internet for commerce. Organized crime is fully operational online, stealing billions of real dollars every year to support worldwide networks of crime, yet the Racketeer Influenced and Corrupt Organizations (RICO), laws do not apply to cyberspace. The Administration has proposed allowing RICO to cover crimes committed in cyberspace, as well as setting mandatory minimum sentences for intrusions into critical infrastructure.

Similarly, recent incidents such as the Sony and Citibank intrusions have highlighted the large discrepancies in our data breach laws. Currently, each state is permitted to regulate when and how a company must disclose a breach of customer data to those affected. This regime makes little sense in cyberspace, where crimes and transactions take place at a national or international level. The Administration's proposals, as well as those introduced in the House and Senate, seek to set a federal standard for data breach notification. As we move to this model, however, we must also take care to implement the most effective -- not the lowest -- standard for reporting.

Finally, we must reexamine new opportunities for voluntary information sharing to ensure that we stop new threats before they reach their target. Today, our system of cyber-defense could be considered a digital Maginot Line. The government, businesses, and citizens all build their own digital fortifications and intruders maneuver to go around them. While the problem of attribution in cyberspace is always an issue, the government has a sophisticated understanding of the dangers we face. It also lacks the visibility of those in the private sector – telecommunications in particular - which can better pinpoint the source of the threat, or even stop it before it reaches our digital doorstep. This system is in place to today to help separate and protect our citizens' private data from being accessed unnecessarily by the government. But as the recent intrusions into Sony and other social networking sites have shown, the bad guys care little about privacy or security. Instead, we are losing the ability to stop attacks before they take place and provide better data security for everyone.

To address this issue without comprising privacy, the Administration proposes allowing cyber threat information to be shared voluntarily with the Department of Homeland Security, so that businesses, private citizens, and the government can all benefit from and be better protected by the increased capabilities and insight of an enhanced public-private partnership. In order for this arrangement to work, we must institute strict oversight to ensure that no personal communications or sensitive data are inappropriately shared with the government by businesses. This effort, if handled carefully and appropriately, could greatly enhance privacy by stopping malicious intrusions or large data theft efforts, and it is already under consideration by other partner countries as a way to provide a clearer picture of the health and security of the internet.

We are reaching critical mass, where our citizens are finally becoming aware of the threats that exist online, but a major catastrophe has not yet fallen on our digital shores. Inevitably, once such an event does occur, there will be strong and irresistible calls for broader measures that could overreact to a new threat. We must act now to implement sensible policies that enhance both security and privacy, before we are faced with a set of decisions that could fundamentally alter one of the most incredible tools of our time. I commend Senator Whitehouse for being a true leader on this issue as both a former member of the Senate Intelligence Committee and now Chairman of this Subcommittee. Thank you Mr. Chairman and Ranking Member Kyl for allowing me to testify today, and I look forward to working with you to help make the internet a stronger and more secure domain for all.

PREPARED JOINT STATEMENT OF JAMES A. BAKER, DEPARTMENT OF JUSTICE; GREG SCHAFFER, DEPARTMENT OF HOMELAND SECURITY; AND ARI SCHWARTZ, DEPARTMENT OF COMMERCE

Statement for the Record
Of

James A. Baker
Associate Deputy Attorney General
Department of Justice

Greg Schaffer
Acting Deputy Undersecretary
National Protection and Programs Directorate
Department of Homeland Security

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology
Department of Commerce

Before the
Committee on the Judiciary,
Crime and Terrorism Subcommittee

Presented:

June 21, 2011

Introduction

Chairman Whitehouse, Ranking Member Kyl, and Members of the Committee, it is an honor for us to appear before you today to discuss the critical issue of cybersecurity. Specifically we plan to address the Administration's legislative proposal to improve cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

The Nation's digital infrastructure is fundamental to our economy, critical to our national security and defense, and essential for open and transparent government. Today, however, the same technologies that empower our citizens and organizations for good can be misused by some for harm.

The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

Although the loss of national intellectual capital is deeply concerning, we increasingly face threats that are of even greater concern. We can never be certain that our information infrastructure will remain accessible and reliable during a time of crisis, but we can reduce the risks.

Recognizing the serious nature of this challenge, the President made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The President also highlighted the importance of sharing responsibility for cybersecurity, working with industry to find solutions that improve security and promote prosperity.

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Through this ongoing work, it has become clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated. We will never be fully insulated from cyber attacks. However, these proposals provide important steps in improving the cybersecurity posture of the United States. Members of both parties in Congress have come to the same conclusion as approximately 50 cyber-related bills were introduced in the last session of Congress. Senate Majority Leader Reid and six Senate committee chairs thus wrote to the President and asked for his input on cybersecurity legislation, while Members from both sides of the aisle have remained steadfast in their resolve to act. The Administration welcomed the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider as it moves forward on cybersecurity legislation. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace.

The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

Protecting the American People

1) National Data Breach Reporting. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus

helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements with a clear and unified nationwide requirement. It also helps ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

2) Penalties for Computer Criminals. The laws regarding penalties for computer crime are not fully synchronized with those for other types of crime. For example, a key tool for fighting organized crime is the Racketeering Influenced and Corrupt Organizations Act (RICO). Yet RICO does not apply to computer crimes, despite the fact that they have become a big business for organized crime. The Administration proposal thus clarifies the penalties for computer crimes, synchronizes them with other crimes, and sets a mandatory minimum penalty for attacks that damage or shut down computers that control our critical infrastructure.

Protecting our Nation's Critical Infrastructure

Our safety and way of life depend upon our critical infrastructure as well as the strength of our economy. The Administration is already working to protect critical infrastructure from cyber threats, but we believe that the following legislative changes are necessary to better protect this infrastructure:

1) Voluntary Government Assistance to Industry, States, and Local Government. Organizations that suffer a cyber intrusion often ask the Federal Government for assistance with fixing the damage and for advice on building better defenses. For example, organizations sometimes ask DHS to help review their computer logs to see when a hacker broke in. However the lack of a clear statutory framework describing DHS's authorities has sometimes slowed the ability of DHS to help the requesting organization. The Administration proposal will enable DHS to quickly help a private-sector company, state, or local government when that organization asks for help. It also clarifies the type of assistance that DHS can provide to the requesting organization.

2) Voluntary Information Sharing with Industry, States, and Local Government. Businesses, states, and local governments sometimes identify new types of computer viruses or other cyber threats or incidents, but they are uncertain about whether they can share this information with the Federal Government. The Administration proposal makes clear that these entities can share information about cyber threats or incidents with DHS. To fully address these entities' concerns, it provides them with immunity when sharing cybersecurity information with DHS. At the same time, the proposal mandates robust privacy oversight to ensure that the voluntarily shared information does not impinge on individual privacy and civil liberties.

3) Critical Infrastructure Cybersecurity Risk Mitigation. The Nation's critical infrastructure, such as the electricity grid and financial sector, is vital to supporting the basics of life in America. Market forces are pushing infrastructure operators to put their infrastructure online, which enables them to remotely manage the infrastructure and increases their efficiency. However, when our infrastructure is online, it is also vulnerable to malicious cyber activities that could cripple essential services. Our proposal emphasizes transparency to help market forces ensure that critical-infrastructure operators are accountable for their cybersecurity.

   The Administration proposal requires DHS, in consultation with the appropriate agencies, to work with industry to identify the Nation's core critical infrastructure and to prioritize the most important cyber risks to that infrastructure. Representatives of critical infrastructure entities and standards setting organizations would then work together to propose standardized risk mitigation frameworks which focus not on compliance but instead on increasing actual security in a cost-effective manner. Then, each critical-infrastructure operator would propose a plan that identifies the steps it will take to address the identified risks as guided by the applicable framework. Each critical infrastructure entity's plan will be assessed by a third-party, commercial evaluator. Companies that are already required to report to the Security and Exchange Commission (SEC) would also have to certify to the SEC that they had developed and were implementing a risk mitigation plan. A high-level summary of the plan and the evaluation results would be publically accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify or produce a new framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial evaluators.

Protecting Federal Government Computers and Networks

Over the past five years, the Federal Government has greatly increased the effort and resources we devote to securing our computer systems. While we have made major improvements,[1] updated legislation is necessary to reach the Administration goals for Federal cybersecurity, so the Administration's legislative proposal includes:

1) Management. The Administration proposal would update the Federal Information Security Management Act (FISMA) and formalize DHS' current role in managing cybersecurity for the Federal Government's civilian computers and networks, in order to provide departments and agencies with a shared source of expertise. The legislation would also promote the ongoing transformation of FISMA toward increased automation and performance based security measures.

2) Personnel. The recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, so we need to be sure that the government can recruit and retain these

[1] *See* GAO, *.Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, March 5 2010.

talented individuals. Our legislative proposal will give DHS more flexibility in hiring these individuals. It will also permit the government and private industry to temporarily exchange experts from the other, so that both can learn from each others' expertise.

3) National Cybersecurity Protection Program. The Administration proposal directs DHS to establish a program to actively protect federal systems and to continue the DHS efforts that are underway in this area. This program will include activities such as deploying intrusion detection and prevention capabilities, conducting risk assessments, and providing incident response and other technical assistance. DHS conducts many of these activities today under existing authority. For example, DHS is deploying what is referred to as the National Cybersecurity Protection System – of which the EINSTEIN intrusion detection and prevention capabilities are a key component. The EINSTEIN system helps block malicious actors from accessing federal executive branch civilian agencies, while DHS works closely with those agencies to bolster their own defensive capabilities. Despite progress in this area, deploying EINSTEIN to new agencies has sometimes been slowed due to the need for lengthy reviews and interagency agreements. To address this issue, the proposal will clarify DHS' authorities to protect federal systems. At the same time, strong privacy and civil liberties protections have been incorporated into the provision to protect the rights of federal employees and other users of federal systems.

4) Data Centers. The Federal Government has embraced cloud computing, where computer services and applications are run remotely over the Internet. Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law.

Protecting Individuals' Privacy and Civil Liberties

The Administration's proposal ensures the protection of individuals' privacy and civil liberties through a framework designed expressly to address the challenges of cybersecurity.

- It requires DHS to implement its cybersecurity program in accordance with privacy and civil liberties procedures. These must be developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All federal agencies who would obtain information under this proposal will follow privacy and civil liberties procedures, developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All monitoring, collection, use, retention, and sharing of information is limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement purposes only with the approval of the Attorney General.
- When a private-sector business, state, or local government wants to obtain immunity in connection with sharing of information with DHS, it must first make reasonable efforts to remove identifying information unrelated to cybersecurity threats.

- The proposal also mandates the development of layered oversight programs and congressional reporting.
- Immunity for the private sector business, state, or local government is conditioned on its compliance with the requirements of the proposal.

Taken together, these requirements create a new framework of privacy and civil liberties protection designed expressly to address the challenges of cybersecurity.

Conclusion

Our Nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress as they move forward on this issue.

QUESTIONS SUBMITTED BY SENATOR SHELDON WHITEHOUSE FOR JAMES A. BAKER, GREG SCHAFFER, AND ARI SCHWARTZ

Questions for the Record Submitted by Senator Sheldon Whitehouse
Subcommittee on Crime and Terrorism June 21, 2011 Hearing, "Cybersecurity: Evaluating the Administration's Proposals"

1. Under the Administration's proposal, a rulemaking process would identify critical infrastructure in the United States. Current legislative discussions presume that the electrical grid and certain other pieces of infrastructure will be determined to be critical in such a rulemaking process. Internet Service Providers (ISPs) would appear to be an essential element of our infrastructure and economy. Should Congress expect ISPs (or elements thereof) to be identified as critical infrastructure under the proposed rulemaking process?

2. Would the Administration's proposal and anticipated regulations enable or require ISPs to notify customers that they are the unwitting and unwilling bearers of viruses, malware and other threats? What steps would the Administration propose to customers whose computers are bearers of viruses, malware, and other threats, particularly to those unwilling to take reasonable remedial and protective steps?

3. Many experts agree that sharing of cybersecurity threat information should be improved. To this end, the Administration proposes allowing increased sharing of cybersecurity threat information with the Department of Homeland Security. Specifically, it proposes excepting such information sharing from existing data privacy and other laws. Please provide examples to explain (a) which data privacy and other laws prevent (b) which actors from sharing (c) what types of cybersecurity information (d) with whom (e) in which situations.

RESPONSES SUBMITTED BY JAMES A. BAKER, GREG SCHAFFER, AND ARI SCHWARTZ

Question#:	1
Topic:	proposal
Hearing:	Cybersecurity: Evaluating the Administration's Proposals
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: Under the Administration's proposal, a rulemaking process would identify critical infrastructure in the United States. Current legislative discussions presume that the electrical grid and certain other pieces of infrastructure will be determined to be critical in such a rulemaking process. Internet Service Providers (ISPs) would appear to be an essential element of our infrastructure and economy. Should Congress expect ISPs (or elements thereof) to be identified as critical infrastructure under the proposed rulemaking process?

Response: The Administration's cybersecurity legislative proposal does not specify which infrastructure will be designated as "covered critical infrastructure" and instead opts for an inclusive and transparent rulemaking process to develop the list. It is premature to commit to which items will or will not be included in a proposed rulemaking.

Question#:	2
Topic:	ISPs
Hearing:	Cybersecurity: Evaluating the Administration's Proposals
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Question: Would the Administration's proposal and anticipated regulations enable or require ISPs to notify customers that they are the unwitting and unwilling bearers of viruses, malware and other threats?

Response: The Administration understands that some internet service providers (ISPs) have already begun pilot projects to better inform customers regarding intrusions into their networks. Although the Department of Homeland Security is supportive of ISPs working with their customers on a voluntary basis to enhance the security of the entire digital ecosystem, the Administration's proposal is silent on the particular issue of ISPs sharing information with customers or other private sector entities to inform them that they are subject to malware or other cybersecurity threats. To the extent that such information sharing is currently permissible, it would continue to be so under the proposal. We look forward to working with the Chairman and members of the Committee to determine if additional action should be taken to encourage this type of assistance.

Question: What steps would the Administration propose to customers whose computers are bearers of viruses, malware, and other threats, particularly to those unwilling to take reasonable remedial and protective steps?

Response: Within the National Protection and Program Directorate's Office of Cybersecurity and Communications, the U.S. Computer Emergency Readiness Team provides government agencies, the private sector, and the general public with suggested cybersecurity best practices and vulnerability and mitigation information. Internet service provider (ISP) customers are encouraged to regularly update anti-virus software, download vendor security patches, and exercise caution when using removable media, following links, or opening email attachments. If an ISP customer is unwilling to implement these remedial and protective steps, those customers should be made aware of the potential associated consequences, such as identity theft, financial fraud, privacy concerns, and the theft of other types of data. ISP customers should be aware of consequence-management resources available to them, such as credit and bank account monitoring, and should also consider limiting the amount of personal information stored or accessed from their computers.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement for the Record of Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

June 21, 2011

Chairman Whitehouse, Ranking Member Kyl, and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record on behalf of the Center for Democracy & Technology[1] about the Administration's proposed cybersecurity legislation.[2] We applaud the Subcommittee for examining these proposals, critical parts of which implicate matters that are within the jurisdiction of the Judiciary Committee, including:

- Data breach notification;
- Amendments to the Computer Fraud and Abuse Act; and
- Cybersecurity information sharing provisions.

Today, I will briefly outline existing threats to our cybersecurity. I will then discuss some of the key distinctions that must be drawn in order to chart a path forward that provides for meaningful improvements in security while ensuring protection for America's cherished rights of privacy and free expression and encouraging continued innovation. I will examine the Administration's cybersecurity proposals in broad strokes, then focus on the three proposals that fit within the Judiciary Committee's jurisdiction. I will suggest an approach to information sharing more likely to protect civil liberties and promote security, explain why the Administration's data breach notification proposal is a good start but needs some modifications, and encourage you to address longstanding concerns with

---

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom. CDT coordinates a number of working groups, including the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies, and trade associations interested in information privacy and security issues.

[2] Text of the White House cybersecurity legislative proposal: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf (hereinafter, "White House proposal") Section-by-section analysis of the proposal, prepared by the White House: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill-Section-by-Section-Analysis.pdf.

the ambiguity and breadth of the CFAA before considering the penalty enhancements the Administration has proposed.

An overarching theme of our statement for record is that Congress should take a careful, nuanced approach when crafting cybersecurity authorities, avoiding overbroad legislation and the attendant unintended consequences to individual rights and technological innovation. In particular, CDT urges the Subcommittee to think carefully about the role of government in enhancing national cybersecurity. Government action is surely required in some areas, but in others government intervention would raise significant civil liberties concerns, could impede innovation, and might be counterproductive from a security standpoint.

The Cybersecurity Threat

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. Earlier this month, the International Monetary Fund (IMF) released news of a major attack on its network that may have given hackers access to the organization's collection of sensitive market data about struggling state economies worldwide.[3] The IMF's announcement came just weeks after one of the nation's largest defense contractors, Lockheed Martin, suffered a "significant and tenacious" cyber attack on May 21.[4] In 2010, the Stuxnet worm, allegedly designed with the involvement of the U.S. government, penetrated the control systems of centrifuges Iran was using to refine uranium, causing hundreds of the centrifuges to spin out of control and damage themselves.[5]

The GAO, among others, has repeatedly criticized the federal government for failing to respond adequately to this threat.[6] The scope of the federal response should not be dictated by the need to react to such criticisms, however, but instead by the actual problems that lie behind them.

---

[3] Sudeep Reddy and Siobhan Gorman, IMF Hit by Cyber Attack, *The Wall Street Journal* (June 11, 2011), http://online.wsj.com/article/SB10001424052702304259304576380034225081432.html.

[4] Gopal Ratnam, U.S. Offers Lockheed Help After 'Tenacious' Cyber Attack, *Bloomberg News* (May 29, 2011), http://www.bloomberg.com/news/2011-05-29/lockheed-offered-help-after-cyber-incident-u-s-government-says.html.

[5] William Broad, et al., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times* (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[6] *See, e.g.*, Testimony of David A. Powner, Director, Information Technology Management Issues, Government Accountability Office, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* (September 13, 2006), *http://www.gao.gov/new.items/d061087t.pdf*. In 2008, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities. Testimony of Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, Government Accountability Office, *Cybersecurity, Continued Federal Efforts Are Needed to Protected Critical Systems and Information* (June 25, 2009), http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/25jun/Wilshusen_Testimony.pdf. In 2010, GAO found continued shortcomings. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (October 6, 2010), http://www.gao.gov/products/GAO-11-24.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. One size does not fit all. There are four important sets of distinctions to be drawn in any attempt to tackle the cybersecurity problem:

- First, a distinction must be drawn between those systems that are government-owned and those that are owned by the private sector.
- Second, distinctions must be drawn based on the degree to which the operation of particular systems is vital to the national well-being.
- Third, systems that support free speech and democratic discourse must be distinguished from those that do not.
- Fourth, threats to systems must be distinguished based on the capabilities and intentions of the originators of those threats.

Keeping these distinctions in mind when tailoring a cybersecurity policy to the needs of various systems is vital.

First, it is absolutely essential to draw appropriate distinctions between military government systems, civilian government systems, and systems owned and operated by the private sector. Policy towards government systems, both those in the military domain and those under .gov, can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

Second, particularly with respect to private systems, it is important to remember that most networks are not critical infrastructure and should not be treated as such. While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the Internet into the same regulatory basket. For example, while it is appropriate to require strong authentication of a user of an information system that contains classified information or controls a critical element of the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

Third, when developing policy responses, appropriate distinctions should be made between the elements of critical infrastructure that primarily support free speech and democratic participation – most prominently the Internet – and those that do not. The characteristics that have made the Internet such a success – its open, decentralized, and user-controlled nature and its support for innovation and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all critical infrastructure. Policies that may be appropriate for the power grid or the banking system may not be appropriate for components of the Internet used for exercising First Amendment rights to speak, associate, and petition the government.

Fourth, any cybersecurity policy must recognize that networked system security is aimed at countering a broad range of threats, from national-level actors engaging in the theft of state secrets to organized criminals engaged in financial fraud to teenage hackers testing their skills. As one cybersecurity expert has noted, it is important to "break down attacks by attribution and

category."[7] Only then can the cybersecurity policy be appropriately tailored to a particular set of threats and not attempt to fit these diverse activities into the same policy framework.

For all these reasons, a sectoral, threat-specific approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet critical to new economic models, human development, and civic engagement are not regulated in ways that could stifle innovation, chill free speech, or violate privacy.

Top Line View of the Administration's Cybersecurity Proposals

The White House's legislative package of cybersecurity reforms is largely balanced and contains some appropriate nuance, but includes some troubling provisions.

As compared to the leading Senate cybersecurity bill (the Cybersecurity and Internet Freedom Act (CIFA), S. 413), the Administration's bill could subject more entities and assets to regulation as "critical infrastructure" but that regulation would have a lighter touch. The White House proposal defines critical infrastructure as those entities and assets whose incapacity or disruption would cause "a debilitating impact."[8] This vague language could encompass a broad swath of industry. CIFA does a better job, defining critical infrastructures as those systems whose disruption would cause "a mass casualty event which includes an extraordinary number of fatalities," "severe economic consequences," "mass evacuations with a prolonged absence," or "severe degradation of national security capabilities, including intelligence and defense functions."[9] On the other hand, CIFA would impose heavier regulatory burdens on those critical infrastructure owners and operators. CIFA would impose fines for non-compliance with key requirements, while the Administration bill would instead use transparency to encourage compliance, by requiring companies to report publicly their compliance failures. CDT favors the tighter definition of "critical infrastructure" in CIFA (though we would tighten it more) and the lighter regulatory hand of the Administration's bill.

Like CIFA, the White House bill properly makes the Department of Homeland Security (DHS) rather than the Department of Defense (DOD) responsible for securing civilian government systems and for working with the private sector to secure privately held critical infrastructure. The Department of Defense would continue to secure classified systems and the .mil domain. This is the best allocation of responsibilities. There is serious concern that if the National Security Agency or another DOD entity were to take the lead role in cybersecurity for civilian unclassified systems or private sector systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, thereby increasing the likelihood of failure and decreasing the effectiveness of the effort. The White House legislation draws the lines of authority appropriately.

The White House bill also wisely omits any provision that would give the President or DHS the

[7] Scott Charney, Rethinking the Cyber Threat: A Framework and a Path Forward 7 (2009) http://download.microsoft.com/download/F/1/3/F139E667-8922-48C0-8F6A-B3632FF86CFA/rethinking-cyber-threat.pdf.

[8] White House proposal, proposed Section 3(b)(1)(A) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[9] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 254 of the Homeland Security Act and amendments to Section 210E of the Homeland Security Act.

authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[10] This is good policy for many reasons. To our knowledge, no circumstance has yet arisen that could justify a governmental order to limit or cut off Internet traffic to a particular privately owned and controlled critical infrastructure system. Operators know better than do government officials whether their systems need to be shut down or isolated. In contrast, a new Presidential "shut down" power comes with a myriad of unexamined risks. Even if such power over private networks were exercised only rarely, its mere existence could enable a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. It would make private sector operators reluctant to share information because it could be used to order them to shut down. Conversely, when private operators do determine that shutting down a system would be advisable, they might hesitate to do so without a government order, and could lose precious time waiting to be ordered by the government to shut down so as to avoid liability for the damage a shutdown could cause others. Finally, the grant of "shut down" authority to the President for cybersecurity purposes would set a precedent other repressive countries would cite when shutting down Internet services for other purposes, including the stifling of dissent. For all of these reasons, we believe it was wise for the Administration to leave this issue out of its bill.

Finally, the White House legislation honors the President's pledge, made in connection with the 2009 release of the Cyberspace Policy Review, that the federal government would not monitor private networks as part of its cybersecurity program.[11] Monitoring private communications networks is the job of the private sector communications service providers themselves, not of the government. Private sector operators already monitor their networks on a routine basis to detect and respond to attacks as necessary to protect their networks.

Nevertheless, caution must be exercised to ensure that government monitoring of private-to-private communications does not occur as an indirect result of information sharing between the private and public sectors or as an unintended by-product of programs put in place to monitor communications to or from the government.

I will now turn to the Administration's information sharing proposal and its other proposals that fall with the Judiciary Committee's jurisdiction.

White House Information Sharing Proposal Is Overbroad, Raising Privacy Concerns

There is widespread agreement that the current level of cybersecurity information sharing – sharing that is essential to a robust cybersecurity program – is inadequate. Private sector network operators and government agencies monitoring their own networks could better respond to threats if they had more information about what other network operators are seeing. How to encourage more robust information sharing without putting privacy at risk is a central policy challenge that falls to the Judiciary Committee to resolve, because many of the statutes

[10] The Cybersecurity and Internet Freedom Act includes such a provision. For an analysis, see http://www.cdt.org/blogs/greg-nojeim/does-senate-cyber-bill-include-internet-kill-switch.

[11] When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama pledged that: *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

that would have to be amended or overridden are within the Committee's jurisdiction.

a. Information Sharing Between the Private Sector and DHS Under the White House Proposal

As a solution to this problem, the White House has proposed a sweeping information sharing regime that would permit any entity to share with DHS any information the entity may have, including communications traffic, no matter how it was acquired, no matter whether it is thought to include information about an attack or not, and *no matter how use and disclosure of that information would otherwise be restricted by law*, so long as the entity shares it for the purpose of protecting a system against a cybersecurity threat, makes reasonable efforts to remove irrelevant identifying information, and complies with as-yet-unwritten privacy protections.[12] The provision would permit a vast amount of personal information to flow to and from DHS and would effectively override protections in the Wiretap Act, the Electronic Communications Privacy Act, the Communications Assistance for Law Enforcement Act, the Foreign Intelligence Surveillance Act, the Freedom of Information Act, the Privacy Act of 1974, and the Sherman Antitrust Act – statutes within the jurisdiction of the Judiciary Committee.[13] In contrast, the leading Senate cybersecurity bill explicitly requires information sharing relating to cybersecurity to adhere to the statutory schemes governing electronic surveillance.[14]

In other words, this "hub and spoke" model of information sharing in the White House bill puts the Department of Homeland Security at the center. DHS would receive information, analyze it, and could share what it receives as well as the results of its analysis with other entities.

On the plus side, information sharing under the Administration proposal would be voluntary, not mandatory. This is commendable because giving a governmental entity mandatory authority to access private sector data that is relevant to cybersecurity[15] would completely eviscerate the electronic surveillance laws and would undermine the public-private partnership that needs to develop around cybersecurity. In addition, it is good to see that the proposal indicates that DHS's policies and procedures must require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to cybersecurity threats.

In other regards, however, the White House proposal raises serious concerns. Most fundamentally, the White House information sharing proposal is based on an unsupported premise: the bill assumes that the government is in the best position to identify threats to private sector networks. Therefore, the proposal would permit the sharing of much Internet traffic with the DHS for analysis. We believe that there is no evidence that the government has either the expertise or the ability to act quickly enough to protect private sector networks better than the private sector can. A better approach is to build on and improve the current network security activities of the private sector. As we explain below in our discussion of an alternative approach to information sharing, much more narrowly targeted changes can be made to the privacy laws. Such changes would promote private sector cooperation for cybersecurity without the risks

[12] White House proposal, "Department of Homeland Security Cybersecurity Authority and Information Sharing, proposed Section 245 of the Homeland Security Act.

[13] It also supersedes any state statute that regulates interception, collection, use, and disclosure of communications.

[14] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c) of the Homeland Security Act.

[15] For an example of such a proposal, see Section 14 of S. 773, the Cybersecurity Act of 2009, as introduced in the 111th Congress.

associated with feeding large amounts of traffic to the government.

Under the White House proposal, DHS could use and retain the communications traffic and other information it receives from service providers, could further disclose that information to private entities and to state and local governmental entities for cybersecurity purposes, and could disclose it to law enforcement entities when it is evidence of a crime. Agencies receiving communications, records, and other disclosures from DHS could use them for cybersecurity and law enforcement purposes and could further disclose them to other entities that have agreed in writing to use them for cybersecurity and law enforcement purposes and to abide by the as-yet-unwritten privacy protections.

The privacy and civil liberties protections in the proposal are weak, difficult to enforce, and principally center on the purpose limitation: limiting information sharing to cybersecurity and law enforcement purposes. Sharing a vast amount of communications traffic could, however, fall within those broadly defined purposes. The legislation would draw no distinctions between sharing content and non-content. While DHS would issue policies and procedures designed to protect privacy and civil liberties, it would have substantial discretion about what to include and little legislative guidance. The proposed legislation does not require that those policies and procedures be subject to notice and comment rulemaking under the Administrative Procedure Act. Moreover, there is no effective way for an aggrieved party to enforce compliance with the policies and procedures because there is no private right of action for violations. Knowing and willful violations are misdemeanors that the Department of Justice has discretion to prosecute; they bring no prison time and fines can be no more than $5,000/incident. Companies and state and local governments that violate the law and share communications and other information for inappropriate purposes, or who fail to strip out irrelevant identifying information, or who violate the privacy policies and procedures, are immune from civil and criminal liability under *all other laws* if they relied in good faith on their own determination that their conduct was permitted in the proposed statute. Finally, the DOJ – a law enforcement agency – would decide which information could be disclosed for law enforcement purposes.

We urge you to assert jurisdiction over cybersecurity information sharing within the purview of the Committee, and to take a more nuanced approach.

b. An Alternative Approach

First, Congress should determine exactly what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[16] and the public-private partnerships represented by the Information

[16] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

Sharing and Analysis Centers (ISACs),[17] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[18] Those suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[19] Industry is now represented at the NCCIC[20] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, Congress must make a realistic assessment as to whether an information sharing model that puts the government at the center – receiving information, analyzing it, and sharing the resulting analysis and even the raw information itself with industry – could ever be the basis for a rapid-response center possessing adequate expertise to effectively protect an overwhelmingly diverse set of private systems and enough speed and flexibility to respond to fast-moving threats. We have serious doubts. An industry-based model, subject to strong privacy protections, might be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a government-centric model.

An information sharing approach that relies on the expertise of network operators would be far less disruptive of the current legal framework. Current law already gives communications service providers authority to monitor their own systems and to disclose both to governmental entities and to their own peers information about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose, or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider.[21] This includes the authority to disclose

---

[17] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established an Information Sharing and Analysis Center (ISAC) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See* The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection 1 (January 2009), http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[18] *See* Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588.

[19] *See* DHS Press Release announcing opening of the NCCIC, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[20] *See* DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full time IT-ISAC analyst at the NCCIC, November 18, 2010, http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.

[21] 18 U.S.C. § 2511(2)(a)(i).

communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications[22] and customer records[23] to any governmental or private entity.[24] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[25] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass.[26]

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Furthermore, the extent of service provider disclosures to the government for self-defense purposes is not known publicly. We urge the Subcommittee to consider imposing a requirement that the extent of such information sharing be publicly reported, in de-identified form, both to assess the extent to which beneficial information sharing is occurring and to guard against ongoing or routine disclosure of Internet traffic to the government under the self-defense exception.

While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, the law does not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. There may be a need for a very narrow exception to the Wiretap Act, ECPA, FISA, and other laws that would permit disclosures about specific attacks and malicious code on a voluntary basis and that would immunize companies against liability for these disclosures.

The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited. It would thus need to focus on the categories of information that many believe are most important to share: cyberattack signatures and attribution data associated with suspected cyberattacks. Under the approach we envision, these narrowly defined categories of information could be shared more widely, permitting service providers to share directly with each other without going through the government. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy. CDT is drafting such an exception and is seeking comment in an effort to ensure that it is effective, is not overbroad, and includes appropriate enforcement and reporting requirements in order to prevent misuse.

Moreover, we urge the Subcommittee, before making any amendments that weaken the controls and privacy protections of the surveillance laws, to consider counterbalancing such

[22] 18 U.S.C. § 2702(b)(3).

[23] 18 U.S.C. § 2702(c)(5).

[24] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. §§ 2702(b)(8) and (c)(4).

[25] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. § 2510(21).

[26] 18 U.S.C. § 2511(2)(i).

changes with legislation to update ECPA by making its privacy protections more relevant to today's digital environment.[27] We would welcome the opportunity to work with the Subcommittee on such legislation.

c. Inter-agency Information Sharing To Prevent Intrusions Into Government Networks

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has the responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that citizens' communication with their government implicates the exercise of the First Amendment rights of free speech and petitioning the government, which will be chilled if communications between Americans and their government are routinely shared with law enforcement and intelligence agencies. While the Fourth Amendment may not be implicated in citizen-to-government communications (because those communicating with governmental entities necessarily reveal their communications – including content – to the government), the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government, whether to access services or to criticize government actions.

The White House proposal puts the responsibility to monitor government civilian networks right where it belongs: on the shoulders of the Department of Homeland Security. Under the bill, DHS is charged broadly with engaging in cybersecurity and information infrastructure protection for civilian government systems in what would become new Sections 243 and 244 of the Homeland Security Act. Among other things, DHS would conduct risk assessments of federal systems and maintain a cybersecurity center that would serve as a focal point for cybersecurity information flowing from other governmental agencies at the federal, state, and local level and from the private sector.

We are concerned, though, about the vast scope of the information that could flow to the DHS cybersecurity center from other federal agencies under the White House proposal. The center would be authorized, notwithstanding any law, to intercept, retain, use, and disclose communications traffic to, from, or on any federal system and to deploy countermeasures that block or modify data packets on an automated basis, for cybersecurity purposes.[28] Communications content could be retained, used, and disclosed for cybersecurity purposes when associated with a known or suspected threat, and disclosed to law enforcement when it constitutes evidence of a crime. Users of federal systems would have to be given notice of the monitoring and potential for onward disclosure, but such blanket, mandatory "consent" is not true consent and does not address the First Amendment and privacy concerns. DHS would issue its own privacy and civil liberties policies and procedures in connection with this program, but there would be no independent oversight or auditing to ensure that only traffic to and from government systems is accessed and that ECPA is not being violated through access to purely private communications. Instead, the Secretary of DHS would annually certify the department's

[27] Specifically, the Judiciary Committee should take up the reforms proposed by the Chairman in the Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011) introduced on May 17. There is widespread support for updating ECPA. Digital Due Process, a coalition of technology companies, communications service providers, academics, think tanks, and advocacy groups spanning the political spectrum, has recommended targeted, reasonable updates to ECPA. *See* www.digitalddueprocess.org. The Center for Democracy & Technology is a leading member of DDP.

[28] White House proposal, proposed Section 244(b) of the Homeland Security Act.

compliance with these provisions. No penalty is specified for violations.

While we recognize the right and responsibility of the federal government to monitor its networks for intrusion, the scope of this authorization and lack of independent oversight give us pause because the legislation appears to authorize significantly more activity than is necessary to facilitate operation of DHS's Einstein intrusion detection and prevention system.[29] At a minimum, Congress should consider requiring information collected by the center to be disposed of after a set period; requiring independent audits to ensure that only communications traffic with the government is acquired, retained, and used; and requiring DHS to provide an assessment of the federal laws that are being overridden to permit this monitoring program.

White House Data Breach Notification Proposal A Good Starting Point

The White House proposal would require business entities that hold "sensitive personally identifiable information" (SPII) about more than 10,000 people to notify such persons when the business entity suffers a cybersecurity breach that results in disclosure of SPII, unless the breach involves no reasonable risk of harm to the individual. The White House data breach notification proposal is similar in many respects to the data breach notification provisions in the Personal Data Privacy and Security Act (S. 1151) that Senator Leahy introduced on June 7, 2011.[30] Both contain the same coverage threshold (business entities holding SPII of at least 10,000 people), the same harm standard that obviates notice only when there is no reasonable risk of harm, and similar enforcement schemes.

Data breach notification serves cybersecurity purposes by encouraging large business entities that hold personally identifiable information to better protect that information. It also helps defend against the theft of identity, a problem that can undermine cybersecurity in some contexts. Because most states have already adopted data breach notification laws, breach notification is already effectively the law of the land.[31] The White House proposal would pre-empt those laws and therefore warrants special scrutiny to protect against eliminating current protections or other unintended consequences. It would wisely permit enforcement by state attorneys general and includes an innovative provision to authorize the Federal Trade Commission to adjust the categories of SPII it is intended to protect.

Data breach notification, however, is primarily a consumer privacy matter that CDT believes should be part of comprehensive consumer privacy legislation. We urge that you not miss the forest for the trees: what is needed is legislation to protect consumer privacy in the online and

---

[29] The Einstein system is designed to detect and interdict malicious communications traffic to or from federal networks. It assesses network traffic against a pre-defined database of malicious signatures and detects and reports anomalies in network traffic. Einstein operates on the network of an ISP providing service to the government instead of operating on the network of the agency being protected, creating a risk that Einstein could monitor communications traffic that is not to or from a government entity. More about the program can be found in the Einstein 2 Privacy Impact Assessment (PIA) (May 19, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf, in the PIA for the Einstein Initiative Three Exercise (March 18, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf, and in legal opinions issued by the Department of Justice concluding that the Einstein program operates lawfully: http://www.justice.gov/olc/2009/e2-issues.pdf (January 9, 2009), and http://www.justice.gov/olc/2009/legality-of-e2.pdf (August 14, 2009).

[30] The data breach notification provisions in the Personal Privacy and Security Act are in Sections 311-322 of the bill, S. 1151.

[31] *See, e.g.,* http://www.cdt.org/policy/congressional-committee-revives-data-security-legislation.

offline world that incorporates the full range of Fair Information Practice Principles. The effort to adopt data breach notification should not undermine the push for baseline consumer privacy legislation. That said, we believe that if Congress does enact federal data breach notification legislation, the White House proposal is a good starting point, although it should be improved as outlined below.

Definition of Sensitive Personally Identifiable Information. The definition in the White House proposal of "sensitive personally identifiable information" should include health data tied to a name or another identifier. Unless this change is made, the bill would pre-empt several state breach notice laws – such as California's[32] – that cover health data linked to the individual's name. The provision empowering the FTC to modify the definition of sensitive information in rulemaking should be retained to help keep the statute up to date as technology evolves, new categories of sensitive data are put at risk, and new identifiers are developed.

Preemption. The White House proposal would override any provision of state law relating to notification by a business entity "of a security breach of computerized data," but it only requires notice of a subset of such breaches: breaches of data containing specifically defined "sensitive personally identifiable information." As a result, for example, given the definitional problem we noted above, notice of breaches involving personally identifiable health data appears to be outside the scope of the proposed notice requirement but within the scope of the preemption section. That one example can and should be fixed in the statute, but the broader problem of the disconnect between coverage and preemption would remain. Preemption of state law should be limited to the data covered by the federal law, permitting states to develop their own laws to address breach of information categories not covered under the proposal.

Notification Trigger. Businesses must notify consumers of data breaches involving SPII under the White House proposal unless the business determines that there is "no reasonable risk of harm or fraud to consumers." Under this formulation, once a company reasonably determines that a breach has occurred, notice is the default and must be given *unless* there is an affirmative finding of no risk. "Harm" should be construed to include reputational harm or embarrassment, and some disclosures of personally identifiable information, such as health information, should be considered harmful per se; with such a construction, the proposal's trigger appears to be effective while avoiding notification regarding truly inconsequential data breaches. We would caution against requiring notification only where harm has occurred or is likely to occur, or only where there was a determination of a significant risk of harm. If a business determines that there is no reasonable risk of harm and that it is not obligated to notify consumers of a breach, the proposal would require the business to submit its risk assessment to the FTC – a critical safeguard for which CDT has advocated.[33]

Delays for Law Enforcement. Under the White House proposal, federal law enforcement agencies can require businesses to delay notification of a breach if the agencies determine that notification would impede a criminal investigation or national security activity. While such a

---

[32] California's data breach law can be found in its Civil Code at Sections 1798.25-1798.29, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29. The White House proposal could also be modified to include an exception, such as is found in California law, specifying that notification is not required for instances of good faith unauthorized access or acquisition of the data by employees or agents of the data holder, provided the data was not further used or disclosed in an unauthorized manner.

[33] http://www.cdt.org/copyright/20090505_data_p2p.pdf.

provision is appropriate, it should limit the duration of the periods of delay (e.g., 30 days) and require written authorization by a senior law enforcement official.

Computer Fraud Law Needs Tightening Before Increased Penalties Are Considered

The White House proposal includes various amendments to the Computer Fraud and Abuse Act (CFAA).[34] The White House seeks to further broaden the reach of the CFAA, eliminate its first-time offender provisions, make CFAA violations RICO predicates, impose for conspiracies and attempts the same penalties imposed for completed acts that violate the CFAA, impose mandatory minimums for some violations, and add real property to the assets that can be forfeited in civil or criminal proceedings for conduct prohibited in the CFAA.

The CFAA has served as an important component of the online trust framework, giving the federal government authority to pursue cybercrimes including hacking and identity theft. However, vague terms in the law have fueled troubling civil actions that have stretched the application of the law well beyond that which Congress intended. That stretching of the law has spread to criminal cases under the CFAA as well, and a number of activities having little to do with the kinds of computer "trespasses" that originally motivated Congress to pass the CFAA are now potential crimes. Before it is further expanded or its penalties increased, the statute needs to be tightened and limited to the type of computer hacking activity it was intended to penalize so that it more clearly focuses on conduct that threatens cybersecurity. Only then should any expansion of CFAA penalty provisions be considered.

The CFAA imposes liability when a person accesses a computer without authorization or in excess of authorization. Courts have differed significantly on the definitions of "access" and "authorization." Some courts have interpreted unauthorized access so broadly that companies, when setting the terms of service few users will ever read, effectively determine what user conduct is "criminal." In *U.S. v. Nosal*,[35] the Ninth Circuit held just two months ago that a company's former employee violated the CFAA when he acquired information from the firm's computer network and then repurposed it for his own use, because the employer had not authorized that type of access to information on its network. This prompted one online publication to headline a story about the case "Appeals Court: No Hacking Required to Be Prosecuted as a Hacker."[36] While such activity might constitute theft, or a breach of an employment contract, it is certainly not the kind of conduct that should be addressed in a cybersecurity statute.

Similarly, in the 2008 Lori Drew case, a Missouri mother who impersonated a teenage boy on MySpace in order to taunt her daughter's teenage rival was charged in California under the CFAA after the girl committed suicide. The prosecutor's theory was that Drew exceeded authorized access because the MySpace Terms of Service did not allow users to create accounts under a false name. A federal judge overturned Drew's conviction under the CFAA.[37] While Drew's actions were reprehensible, they did not constitute "hacking" in any meaningful

[34] 18 U.S.C. § 1030.

[35] C.A. 9, 10-100038, April 28, 2011

[36] David Kravetz, Appeals Court: No Hacking Required to Be Prosecuted as a Hacker, *Wired: Threat Level* (April 29, 2011), http://www.wired.com/threatlevel/2011/04/no-hacking-required.

[37] The brief in which CDT joined in the Lori Drew case can be found here: http://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf.

sense. Indeed, if violations of terms of service were per se violations of the CFAA, literally millions of otherwise law-abiding Americans could be subject to criminal prosecution for signing up for a service using a false name, misrepresenting their ages, or exceeding limits on storage capacity. Given that the Ninth Circuit called the result in *Drew* into question with its decision in *Nosal*, further prosecutions for this kind of terms of service violation may well happen.

Meanwhile, plaintiffs in civil cases continue to argue for an *even broader* understanding of unauthorized access. In one recent case, a pregnant mother who sued her employer for pregnancy discrimination was countersued under the CFAA for what the company asserted was unauthorized access to its computer systems: "excessive Internet use" in violation of its acceptable use policy.[38] In another, Sony sued users of its PlayStation devices under the CFAA for tinkering with their own lawfully purchased video game consoles without authorization from the in-box license.[39] Just as early civil cases on contractual authorization led to the questionable prosecutions in Nosal and Drew, so too do these cases point the way to additional dubious uses of the CFAA.

Instead of addressing this vexing problem of overbreadth, the White House proposal would enhance CFAA penalties, encouraging more questionable prosecutions. Penalties for first-time offenders would be increased and in some cases more than doubled. A new mandatory minimum three-year sentence would be imposed on those who, as a component of a felonious violation of the CFAA, damage or attempt to damage a critical infrastructure computer, as long as such damage would "substantially impair" the operation of that computer. The CFAA used to have mandatory minimum sentences, but they were repealed in Section 814(f)[40] of the USA PATRIOT Act in a section captioned "Deterrence and Prevention of Cyberterrorism." Before considering new mandatory minimums, an assessment should be made as to why the old ones were repealed.[41]

The White House proposal also makes the CFAA a RICO predicate – adding it to the list of crimes that can be used to demonstrate a "pattern of racketeering activity" to which severe criminal penalties could be applied. Notably, listing a crime under RICO allows civil plaintiffs to sue for triple damages for violations of that crime.[42] Because of the vagueness of the law, making the CFAA a RICO predicate could have the unintended consequence of making legitimate businesses subject to civil RICO suits for routine and normal activities. While such lawsuits may be legally groundless, their reputational impact and the prospect of treble damages and attorneys fees will often drive legitimate businesses into settling unsustainable charges. Moreover, such lawsuits would intensify the feedback loop between civil and criminal

---

[38] *Lee v. PMSI, Inc.*, 2011 WL 1742028 (M.D.Fla. 2011).

[39] Orin Kerr, Today's Award for the Silliest Theory of the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (January 13, 2011), http://volokh.com/2011/01/13/todays-award-for-the-lawyer-who-has-advocated-the-silliest-theory-of-the-computer-fraud-and-abuse-act/.

[40] This section required the U.S. Sentencing Commission to "amend the Federal sentencing guidelines to ensue that any individual convicted of a violation of [18 U.S.C. § 1030] can be subjected to appropriate penalties, without regard to any mandatory minimum term of punishment." It also increased potential maximum penalties under the CFAA and broadened the conduct to which it applied.

[41] Orin Kerr, Congress Considers Increasing Penalties, Adding Mandatory Minimum Sentences to the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (May 24, 2011), http://volokh.com/2011/05/24/congress-considers-increasing-penalties-adding-mandatory-minimum-sentences-to-the-computer-fraud-and-abuse-act/.

[42] 18 U.S.C. § 1964(c).

law that has led to the current overbreadth on the criminal side: as civil plaintiffs, newly incentivized to sue under the CFAA, continue to take novel theories to court, the set of activities which are considered criminal will likely continue to expand.

Finally, the proposal adds "real property" to items subject to civil forfeiture, as long as that property was used or was intended to have been used to commit or facilitate the crime. This would subject to forfeiture the house of the parents of a teenage hacker who has used a computer to attempt to break into someone's network if the parents were aware of this conduct.

The conduct constituting a violation of the CFAA must be narrowed before Congress considers legislation to extend the statute and enhance the penalties under it. As Professor Orin Kerr has suggested, the statute would be significantly improved by clarifying the definition of "authorization" to state that only actions exceeding *code-based* authorization are sufficient to constitute a violation.[43] Clarifying the meaning of "access" and "damage" under the statute would help as well. Even with such changes, however, some of the administration's proposals, such as mandatory minimum sentences for certain CFAA violations, would continue to raise concerns.

Conclusion

We appreciate the opportunity to testify about the White House cybersecurity proposals. They raise critical issues that fall squarely within the Judiciary Committee's jurisdiction and within the jurisdiction of the Subcommittee. We urge you to assert jurisdiction where appropriate, and we look forward to working with you to make progress on these important matters, while at the same time protecting the privacy rights of Americans.

[43] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 *N.Y.U. L. Rev.* pp. 1596-1668 (November, 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740.

STATEMENT OF

THE FINANCIAL SERVICES ROUNDTABLE

SUBMITTED TO THE

SUBCOMMITTEE ON CRIME AND TERRORISM OF
THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

JUNE 21, 2011

This statement is provided on behalf 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 one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

The comments below are intended to briefly describe cybersecurity and data protection in financial services, and the reasoning behind our support of the Administration's May 12 cybersecurity proposal. Thank you for your efforts on the cybersecurity issue and for considering our input.

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 all of this institution-level and industry-level effort is voluntary – not driven primarily by regulation – it is not seen by industry executives as discretionary 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, self-regulatory organizations and government agencies codify and enforce a comprehensive 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 fifty-two institutions, utilities and associations actively partners with the seventeen 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 the Committee to the April 15, 2011 testimony of FSSCC Chair Jane Carlin before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Homeland Security Committee.) 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 thirteen 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.

Obama 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 legislation 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 Law Enforcement title refers to damage to critical infrastructure computers, but also specifically to mail fraud and wire fraud. 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. We urge the Committee and the full Congress to leverage existing financial services protections and circumstances, and their analogs in other sectors, while preserving the inter-sector quality of the proposal.

The remainder of this statement will be structured as a brief commentary on a few key provisions of the proposal.

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 (please see the 2005 FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice), this migration will require both strong pre-emption and reconciliation to existing regulations and definitions of covered data. 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 section 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, Homeland Security's 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.

Conclusion

Because The Financial Services Roundtable is fully committed to advancing cybersecurity and resiliency:

- We will continue to strengthen security with our members and partners,
- We will help answer this question of ecosystem/sector balance,
- And we will work to pass and implement the Administration's cybersecurity proposal.

Thank you once again for your attention to this important issue. If you have any questions regarding this statement, or if we can be of any help to the Committee, please contact:

Leigh Williams

BITS President
The Financial Services Roundtable
1001 Pennsylvania Avenue NW, Suite 500 South
Washington, DC 20004

202 589-2440
leigh@fsround.org

Financial Services Cybersecurity Policy Recommendations
Financial Services Sector Coordinating Council – April 15, 2011

Policy Approaches the FSSCC Supports:

- Federal leadership on a national cyber-security 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 cyber-security supply chain management and promotion of cyber-security 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 cyber-security 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 cyber-security 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.