CYBERSECURITY: INNOVATIVE SOLUTIONS TO CHALLENGING PROBLEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 25, 2011

Serial No. 112–38

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
66–541 PDF WASHINGTON : 2011

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

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
[Vacant]

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
[Vacant]

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON INTELLECTUAL PROPERTY, COMPETITION, AND THE INTERNET

BOB GOODLATTE, Virginia, *Chairman*
BEN QUAYLE, Arizona, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
SANDY ADAMS, Florida
[Vacant]

MELVIN L. WATT, North Carolina
JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
[Vacant]

BLAINE MERRITT, *Chief Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

MAY 25, 2011

CYBERSECURITY: INNOVATIVE SOLUTIONS TO CHALLENGING PROBLEMS

WEDNESDAY, MAY 25, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:03 a.m., in room 2141, Rayburn Office Building, the Honorable Bob Goodlatte (Chairman of the Subcommittee) presiding.

Present: Representatives Goodlatte, Quayle, Coble, Issa, Chaffetz, Griffin, Marino, Adams, Watt, Conyers, Lofgren, and Jackson Lee.

Staff present: (Majority) Vishal Amin, Counsel; Olivia Lee, Clerk; and (Minority) Stephanie Moore, Subcommittee Chief Counsel.

Mr. GOODLATTE. Good morning. The Subcommittee on Intellectual Property, Competition, and the Internet will come to order.

And I will recognize myself for an opening statement.

Today we are holding a hearing on cybersecurity. This is a complex issue that cuts across several Federal agencies and connects a multitude of stakeholders. The issue may be complex, but the consequences of failure are fairly direct.

The Federal Government's computers are attacked by hackers, many from abroad, on a regular basis. Though most of these attacks are thwarted, some end up breaking through. And not all of these attacks are sophisticated. Sometimes it is the low-tech attack that wreaks the most damage as demonstrated by the WikiLeaks case where thousands of classified State Department documents were released online. Had basic cybersecurity practices been followed, it would not have been possible for someone to remove such a large volume of data from those classified computers.

Despite the fact that the Federal sector grabs the headlines, in many respects it really is the private sector that stands on the front lines of cybersecurity. More than 90 percent of our Nation's critical infrastructure is operated by the private sector. Even though the Federal Government has an important role to play, we need to make sure we hear from the private sector and ensure that their hands are not tied due to obtuse regulations and increased bureaucracy.

In 2004, worldwide economic damage from digital attacks was between $46 billion and $56 billion, according to a Congressional Research Service estimate. In 2009, the Administration's cyber-

space policy review estimated that losses from data theft in 2008 were as high as $1 trillion. It is clear that the stakes are high and we must take steps to bolster our cybersecurity now.

Again, while the Government has a crucial role to play, any policy to improve private-sector cybersecurity should not run against or impede our economic prosperity. Regulatory mandates are unlikely to lead to private-sector cybersecurity improvements and will likely hinder economic growth.

The regulatory process is a slow one, whereas the escalating cyber threats our country faces are extremely dynamic problems. Cybersecurity threats and online technologies change quickly, so quickly that any regulations for cybersecurity could be outdated by the time they are finalized.

Further, a burdensome regulatory framework that increases costs for U.S. businesses puts them at a distinct competitive disadvantage to their foreign competitors. Likewise, any efforts by the Government to take control of the Internet through a kill switch should be strongly resisted. The idea of a kill switch harkens to the type of control abused by dictators, as we most recently saw in Egypt.

I believe that Congress and the Administration need to set general parameters and then look for ways to encourage the private sector to do more to protect its infrastructure from cyber attacks. However, in doing so, we need to ensure that a one-size-fits-all mandate from the Federal Government is avoided. Entangling companies in a morass of red tape will not solve the problem and will actually stifle innovation. Companies are on the front lines in this fight, and the private sector is the best equipped to match the increasingly sophisticated threats to our cybersecurity with sophisticated counter-efforts. To be successful, any solutions in this area must unleash the creativity and resourcefulness of the private sector to combat the problem.

One way to accomplish this would be to provide limited liability protection to companies that take steps to improve their cybersecurity capabilities. Providing civil liability safe harbors to businesses that demonstrate compliance with cybersecurity best practices would encourage the private sector to adopt effective measures.

Additionally, I believe that Government has a role to play in public engagement, working with companies to help them understand and appreciate the potential losses that can occur through a cyber intrusion. When folks better understand the potential ramifications, it becomes clearer that it is in their best economic interest to improve their cybersecurity capabilities. Part of this public/private engagement means that companies will need to share experiences and best practices to help identify vulnerabilities and solutions.

As we look at these innovative solutions, I think that we also need to examine the criminal code to ensure that our laws track with the threats posed by hackers and other cyber criminals. Our Nation's law enforcement agencies should have the necessary tools to investigate, apprehend, and prosecute cyber criminals.

Though these ideas are not exhaustive, I think this framework will help us steer the debate toward solutions that address the

complex and challenging problems posed in the cybersecurity sphere. I am currently working on legislation along these lines and look forward to continuing to work with Members of this Committee and industry on that effort.

I look forward to hearing from all of our witnesses today and hope that we can have a spirited discussion on the Administration's cybersecurity proposal and the best steps Congress can take to ensure that our security in the digital era is strong and effective.

And now it is my pleasure to recognize the Ranking Member of the Subcommittee, the gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman. I appreciate the Chairman convening this hearing. I am little disappointed that we don't have our colleagues here from the Crime Subcommittee, especially in light of the Chairman's last few paragraphs suggesting that this may be more readily addressed by dealing with the issue on the criminal side. But I am sure there are other implications here and I am happy to try to explore them hopefully without being as firm in my opinions yet since I am not an expert in this area as the Chairman seems to be. I am not sure that I think the private sector can solve every public problem we have, but that is a subject of a long debate in many, many different contexts.

The protection and security of our Nation's digital information infrastructure is among the highest priorities we face as the transformation of global communications networks to cyberspace continues. As the Administration noted over 2 years ago in its cyberspace policy review, quote, cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and likely regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. Closed quote.

The Administration's answer to these challenges was released last week, and I commend the Chairman for scheduling this hearing promptly so that we can begin to debate these issues in earnest.

Over the past few years, news reports of breaches in the digital security of our businesses, for example, Google, Sony, and PlayStation, or breaches of the digital security of the Government have increased at an alarming rate. Although WikiLeaks has become the face of security breaches within the Government, the more significant breaches are those where Government computers are attacked and infected with malicious code, as was the case last fall when a foreign intelligence agency using a flash drive spread a rogue program through a military computer network of classified and unclassified data.

Various officials and commentators have sounded a clarion call for Congress to address this threat or risk a sophisticated cyber attack that could cripple the U.S. computer networks, including our financial institutions, energy, and electricity systems and transportation networks.

Others have rightly highlighted the fact that we must continue to value individual privacy as we develop effective protocols to secure our digital infrastructure from attack.

The Administration's proposal has been met with mixed reviews. On the one hand, the proposal seems to have received a generally positive reception in the Senate, but at least one critic and former Bush administration official has dubbed the proposal as less than "weak tea," saying "I would call this weak tea except the teabag doesn't seem to have actually touched the water. The privacy and business groups that don't want to do anything serious about the cybersecurity crisis have captured yet another White House."

I am hopeful that both panels today can provide us with a response to that criticism.

In closing, let me say I look forward to learning more about the aims of the Administration's proposal but must note one concern that I am sure Ranking Member Bobby Scott of the Crime Subcommittee and I would share: the inclusion in the proposal of mandatory minimums. Particularly in an area rife with adolescent mischief, it seems to me that there may be missed opportunities if there is no flexibility to educate and take advantage of the genius, albeit sometimes misguided or manipulated, of our youth who may not know that they are committing a cyber crime.

We have two impressive panels today, so I will yield back and look forward to their testimony. Thank you, Mr. Chairman.

Mr. GOODLATTE. I thank the gentleman.

And the Chair is pleased to recognize the Ranking Member of the full Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Goodlatte and our Ranking minority Member, Mel Watt.

I want to join in the request that the Subcommittee on Crime have hearings on this subject since we are not doing it together, and I think it is better that we do it separately anyway, but especially with this mandatory minimum in here.

Now, there may be a mandatory minimum that I like, but I have never met one yet. And to be putting this in, rushing this in without ever clarifying what it is we are putting a mandatory minimum on is not a good way for a Committee on the Judiciary to proceed. And so I think we ought to take that out, and I think that ought to belong to the Subcommittee on Crime to help us get to that.

Now, I am going to be drafting a national law that doesn't have that in it but that will be a lot more particular, and I am hoping that we can get to this. California has the strongest laws on the subject, and I think it is very important. But I don't think that we can do this without taking into consideration some of the other State laws. And I think there has to be one law that supersedes all the State laws unless we have some particular kinds of carve-out that would allow some of them to exist. That is the question I am interested in today. Should we have a national law or should we have exceptions within the national law?

And I will yield back the balance of my time, Chairman Goodlatte. Thank you.

Mr. GOODLATTE. I thank the gentleman.

And I want to assure both the gentleman from North Carolina and the gentleman from Michigan that while the Administration's proposals are deserving of very careful consideration, there will be, I want to assure you, no rush to judgment on them with or without mandatory minimums.

We have two very distinguished panels of witnesses today, and each of the witnesses' written statements will be entered into the record in its entirety. I ask that each witness summarize his testimony in 5 minutes or less, and to help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, it signals that your time has expired.

Before I introduce our witnesses, I would like them to stand and be sworn.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you. You can be seated.

Our first witness is Mr. James Baker. Mr. Baker serves as Associate Deputy Attorney General in the Department of Justice. Mr. Baker is responsible for a range of national security, cybersecurity, and other matters. He 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. In addition, he served as a Federal prosecutor with the Department's Criminal Division from 2008 to 2009. Mr. Baker was Assistant General Counsel for National Security at Verizon Business. He has also taught national security at Harvard Law School and was a fellow at the Institute of Politics at Harvard's Kennedy School of Government. He is a graduate of the University of Notre Dame and the University of Michigan Law School.

Our second witness is Mr. Greg Schaffer. Mr. Schaffer serves as Assistant Secretary for Cyber Security and Communications at the Department of Homeland Security. Mr. Schaffer works within the National Protection and Programs Directorate to lead the Department's cybersecurity efforts. He works with public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm the Nation's strategic cyber and communications infrastructure. Mr. Schaffer previously served as Senior Vice President and Chief Risk Officer for Alltel Communications. Before joining Alltel, Mr. Schaffer worked at PricewaterhouseCoopers and served as a prosecutor at the Department of Justice. He received his B.A. from George Washington University and his J.D. from the University of Southern California Law Center.

Our third witness is Mr. Ari Schwartz. Mr. Schwartz serves as Senior Internet Policy Advisor for the National Institute of Standards and Technology, NIST, at the Department of Commerce. As part of the Commerce Department's Internet Policy Task Force, he provides input on areas such as cybersecurity, privacy, and identity management. He also works on IT-related issues for the White House Office of Science and Technology Policy Cross Agency Working Groups. Mr. Schwartz came to NIST on August 30, 2010 after serving over 12 years as Vice President and Chief Operating Officer of the Center for Democracy and Technology. At CDT, Mr. Schwartz worked to improve privacy protections in the digital age and expand access to Government information via the Internet. He also led the Anti-Spyware Coalition, anti-spyware software companies, academics and public interest groups dedicated to defeating

spyware. He was also named one of the top five influential IT security thinkers of 2007 by Secure Computing magazine.

Welcome to you all and we will begin with you, Mr. Baker.

TESTIMONY OF JAMES A. BAKER, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. BAKER. Good morning, Mr. Chairman, Ranking Member Watt, and Members of the Committee. Thank you for the opportunity to testify today on behalf of the Department of Justice regarding the Administration's cyber legislation proposals.

As the President has stated and as this Committee well knows, the United States confronts serious and complex cybersecurity threats. Our critical infrastructure is vulnerable to cyber intrusions that could damage vital national resources and put lives at risk. Intruders have stolen confidential information, intellectual property, and substantial amounts of funds.

Cyber crime is on the rise and criminal syndicates are operating with increasing sophistication to steal from innocent Americans. Even more alarming, these intrusions might be creating future access points through which criminal actors and others can compromise critical systems during times of crisis or for other nefarious purposes.

Over the past few years, the Government has made real progress in confronting these threats. At the Justice Department, our investigators and prosecutors have established new units such as the National Cyber Investigative Joint Task Force, or NCIJTF, to pull together the resources of many different agencies to investigate and address cyber threats.

Despite the good work that has been going on in this area, the problem is far from resolved. It is clear that new legislation can improve cybersecurity in a number of critical respects as described in the Administration's legislative proposal. I would like to take a moment to highlight two parts of the Administration's legislative package that is aimed at protecting Americans from cyber crime.

First, data breach notification. Data breaches frequently involve the compromise of sensitive, personal information and expose consumers to identity theft and other crimes. Right now, there are 47 different State laws requiring companies to report data breaches in different situations and through different mechanisms.

The Administration's data breach proposal would replace those 47 State laws with a single national standard applicable to all entities that meet the minimum threshold set forth in the proposal. If enacted into law, this proposal, we believe, would better ensure that companies notify consumers promptly when sensitive personally identifiable information is compromised and that they inform consumers about what they can do to protect themselves. The proposal would empower the Federal Trade Commission to enforce the reporting requirements. It would also establish rules for what must be reported to law enforcement agencies when there is a significant intrusion so that, for example, the FBI and the U.S. Secret Service can work quickly to identify the culprit and protect others from being victimized. The national standard would also make compliance easier for industry, we believe, which currently has the bur-

den of operating under the patchwork of all these different State laws that I mentioned.

Second, the Administration's proposal includes a handful of changes to a variety of criminal laws aimed at ensuring that computer crimes and cyber intrusions can be investigated and punished in the same way and to the same extent as other similar or analogous criminal activity. Of particular note, the Administration's proposal would make it clearly unlawful to damage or shut down a computer system that manages or controls a critical infrastructure, and it would establish minimum sentence requirements for such activities. This narrow, focused proposal is intended to provide strong deterrence to this class of very serious, potentially life-threatening crimes. Moreover, because cyber crime has become a big business for organized crime groups, the Administration's proposal would make it clear that the Racketeer Influenced and Corrupt Organizations Act, or RICO, applies to computer crimes.

Also, the proposal would harmonize the sentences and penalties in the Computer Fraud and Abuse Act with other similar laws. For example, acts of wire fraud in the United States currently carry a maximum penalty of 20 years in prison, but violations of the Computer Fraud and Abuse Act involving very similar behavior carry a maximum of only 5 years.

Mr. Chairman and Members of the Committee, this is an important topic and thank you for holding this hearing today. The country is at risk and there is much work to be done to better protect critical infrastructure and stop computer criminals from victimizing and threatening Americans.

I look forward to answering your questions today, and thank you, Mr. Chairman.

[The joint prepared statement of Mr. Baker, Mr. Schaffer, and Mr. Schwartz follows:]

Statement for the Record
of

James A. Baker
Associate Deputy Attorney General
Department of Justice

Greg Schaffer
Assistant Secretary for Cyber Security and Communications
National Protection and Programs Directorate
Department of Homeland Security

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

Entitled:
"Cybersecurity: Innovative Solutions to Challenging Problems"

Before the
Committee on Judiciary
Intellectual Property, Competition and the Internet Subcommittee
United States House of Representatives
Washington, DC

Presented:

May 25, 2011

Introduction

Chairmen Goodlatte and Sensenbrenner, Ranking Members Watt and Scott, 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] *See* GAO, *.Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, March 5 2010.

1) Management. The Administration proposal would update the Federal Information Security Management Act (FISMA) and formalize DHS's 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 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.

Mr. GOODLATTE. Thank you, Mr. Baker.
Mr. Schaffer, welcome.

TESTIMONY OF GREG SCHAFFER, ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS (CS&C), NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. SCHAFFER. Thank you, Mr. Chairman, Ranking Member Watt, and Members of the Subcommittee. It is a pleasure to be here this morning and an honor to be able to testify on this important topic.

No security issue is more pressing to the Nation than cybersecurity today. We face known and unknown vulnerabilities that are being exploited by an expanding set of threat actors with strong and rapidly expanding threat capabilities. They are acting in an environment where we have limited awareness of what they are exploiting on our networks, but through the limited visibility we do have, we know one fact, which is that in cyberspace, offense wins and defense tends to lose. As a consequence, personal privacy is routinely invaded, intellectual property of American companies is continuously siphoned off to points unknown, and as we attach more and more of our critical infrastructure to the networks for the efficiency that they can bring, the power grid, the financial sector, transportation networks, we put more and more of our systems at risk to attacks that can literally impact our way of life. This is a national security issue. It is an economic security issue, and it is a homeland security issue.

We believe that government, industry, and individuals working together will be necessary in order to reform our practices in order to execute a solution to these problems, and the Administration's proposal recently submitted to Congress is designed to do that.

I will focus my comments on two parts of the proposal, one focused on protecting the Federal Government and the other on protecting critical infrastructure.

Under the heading of protecting the Federal Government, the proposal would solidify DHS's responsibilities with respect to leading protection for Federal civilian networks. It would establish protection service capabilities like intrusion detection and intrusion prevention, red teams, and risk assessments for Federal Departments and agencies. It is some of the work that we are already doing today, but it clarifies our authority and it removes the necessity to enter into complicated legal agreements and arrangements in order to execute in our mission space.

It also would modernize the Federal Information Security Management Act, or FISMA. It is similar to many bills that have been presented over the last couple of years to go away from paper-based compliance exercises and move in the direction of real risk reduction through continuous monitoring and operational improvements.

We would also be ensuring that DHS has the cybersecurity hiring authorities in order to get the best people in order to execute in this mission space. As you know, it is extremely competitive to hire people in this space. DOD had some authorities that allows them to move more quickly to do the hiring and pay arrangements that the private sector often can pay more and hire faster. This would simply expand DOD's existing capabilities and apply them to DHS.

Under the heading of protecting critical infrastructure, we believe that the proposal enhances collaboration with the private sector through both voluntary and mandatory programs as well as improving the opportunities for information sharing.

Under the heading of voluntary assistance, it enables DHS to quickly work with the private sector, State, local, tribal, and territorial governments by clarifying our legal authority to provide certain kinds of assistance, including alerts and warnings, risk assessments, onsite technical support, and incident response.

For information sharing, it again clarifies the authority of businesses, State, local, tribal, and territorial governments to provide information that they learn about through operating their own networks which can be useful to help cybersecurity for the Nation. That would be done with immunity when the sharing is done, but it would also be done under mandates for a robust privacy oversight and controls.

Mandatory parts of the provision in the bill would really focus on critical infrastructure mitigation of risk. In this space, the plan is to work with the private sector to develop the kinds of entities that would need to be covered as critical infrastructure to develop frameworks to identify risks, mitigate those risks, and then have the individual companies come up with plans to apply those frameworks to their infrastructure. We would then be able to make that information available to the marketplace. We would also be in a position to get notices of breaches when they happen so that we can have situational awareness across the ecosystem, as well as being able to provide assistance to those companies when breaches do occur.

We believe that these provisions will help improve security across the entire ecosystem, and I thank you again for the opportunity to testify and I stand ready to answer your questions.

Mr. GOODLATTE. Thank you, Mr. Schaffer.

Mr. Schwartz, welcome.

TESTIMONY OF ARI SCHWARTZ, SENIOR INTERNET POLICY ADVISOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. SCHWARTZ. Thank you, Chairman Goodlatte, Ranking Member Watt, Representative Conyers. Thank you for inviting me to testify 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 seeks to protect and while also protecting the privacy and civil liberties of the public.

I will briefly address five parts of the proposal: first, creating secure plans for covered critical infrastructure; second, promoting secure data centers; third, protecting Federal systems; fourth, data breach reporting; and fifth, privacy protections.

One of the most important themes of the proposal is accountability through disclosure. In requiring creation of security plans,

the Administration is promoting the use of private sector expertise and innovation over top-down Government regulation.

The covered critical infrastructure entities will take the lead in developing frameworks of performance standards under the proposal and, therefore, will look to create these frameworks working together with industry and can also ask NIST to work with them to help create these 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 they will not need to invest the resources of taking an intensive approach through developing a Government-mandated framework unless the industry fails to act.

Rather than substituting the Government's judgment for private firms, the plan holds the covered entities accountable to the consumers and the marketplace. This encourages innovation in mitigation strategies, improving adherence to best practice by facilitating greater transparency, understanding, and collaboration.

In that same spirit, the Administration also seeks to promote cloud services that can provide more efficient service and better security to Government agencies and to small businesses and a wide range of other businesses. To do so, the draft legislation proposes to prevent States from requiring companies to build their data center within that State except where expressly authorized by Federal law.

The proposal also clarifies roles and responsibilities for setting Federal information security standards. Importantly, the Secretary of Commerce will maintain the responsibility for promulgating standards and guidelines which will continue to be developed by NIST in cooperation with the private sector.

My colleague from the Justice Department, Mr. Baker, went into great detail about the data breach reporting standard. On that I will just highlight a few pieces.

First of all, we have learned quite a bit from the States, selecting and augmenting those strategies and practices we felt most effective in protecting 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 that they receive, why they are receiving them, and to take action upon them once they receive them.

Also, the Department of Commerce last year held a notice of inquiry under the Internet Policy Task Force set up by Secretary Locke, and through that notice of inquiry, we received many, many comments from a wide range of businesses. They were unified in their stance that a nationwide standard for data breach will make compliance much easier for all those businesses that must follow the 47 different legal standards today.

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 the privacy protections for information collected by and shared with the Government for cybersecurity purposes. The framework would be created in consultation with privacy and civil liberties experts and the Attorney General, subject to regular reports by the Department

of Justice Privacy Office working with the Department of Homeland Security 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 and I do look forward to answering your questions.

Mr. GOODLATTE. Thank you, Mr. Schwartz.

I will recognize myself for a few questions, and I will direct this first one to all of you. What new tools will law enforcement get in the Administration's proposal to investigate and prosecute cyber intrusions and other cyber crimes? I will start with you, Mr. Baker.

Mr. BAKER. Thank you, Mr. Chairman.

So the first thing, as I mentioned in my opening, was a proposal to create and make a clear crime with respect to efforts, either completed efforts or attempted efforts, to damage critical infrastructure systems, and in situations where the damage causes substantial impairment of the systems. So that is one. That is the one that would have the mandatory minimum provision in it, and I can come back to that if you wish.

The other thing is our experience has shown that increasingly cyber crimes are committed by groups of people that are organized. So they are organized criminal activity. And we think, under those circumstances, it is appropriate to make clear that we can use the tools available to us under the Racketeer Influenced and Corrupt Organizations Act, or RICO, to go after those people. They pose a significant threat to the country. They are well organized, and they are effective in terms of being able to steal lots of money and compromise information from lots of people.

The other thing we believe is this will harmonize and bring more, I guess, uniformity to parts of the criminal code with respect to the penalty provisions.

So those are some of the key things that we are looking at here. If I can just come back to the first one that I mentioned, the damage to critical infrastructure systems.

Our objective there is deterrence. What we are focused on is trying to prevent people—encourage people to not engage in those types of activities. That is what we are really after in that situation because when you have damage to a critical infrastructure system, people are going to be harmed, and that is what we want to avoid through these tools.

Mr. GOODLATTE. Thank you.

Mr. Schaffer?

Mr. SCHAFFER. Yes, Mr. Chairman. I won't speak to the particular provisions that Mr. Baker mentioned, but I will say from a Department of Homeland Security perspective, the improved situational awareness that we would expect through the clarity of the voluntary provisions to ask for and get assistance, to have information sharing from the private sector, and the clarity around what the Federal Departments and agencies can disclose and report will, I think, improve the situation for law enforcement across the board. We work cooperatively today with law enforcement agencies

within the Department of Justice, within DHS, and otherwise, and that growing interagency cooperation to know what is happening in the ecosystem I think benefits law enforcement. It benefits network defense. It is good across the entire ecosystem.

Mr. GOODLATTE. Thank you.

Mr. Schwartz?

Mr. SCHWARTZ. I will just briefly add. My two colleagues covered the main areas, but briefly just to give kind of more of a general overview, really the goal is to get the incentives right. We have to make sure that we have a deterrence for those that are doing wrong, that criminals do pay for their crimes, and that companies and entities that need to do the right thing in the space have incentive to do so as well. We think that this package moves us further in that direction. We are happy to work with you further to make sure that we have those incentives right.

Mr. GOODLATTE. Thank you.

The Administration's proposal appears to mandate technical standards for almost any aspect of the private sector. Should the American people feel comfortable with giving the Homeland Security Department the ability to designate any enterprise as covered critical infrastructure? And subject to DHS mandates, are there any avenues for an enterprise to appeal their classification? Mr. Schaffer?

Mr. SCHAFFER. Yes, Mr. Chairman. Thank you for the question.

I think that the way that the statute is set up, that process of identifying critical infrastructure would be done through a rulemaking, and because it would be done through a rulemaking, the private sector would have an opportunity to participate in the process, to comment on the criteria that would be established in order to identify which entities should be a part of critical infrastructure, and then would be in a position to participate in the process of identifying both the risks that needed to be mitigated, the frameworks for mitigation of those risks, and then develop plans to execute on that risk mitigation. So they have got significant roles in the private sector. This is not DHS going out and doing it on its own.

Mr. GOODLATTE. Right, but if they want out, can they get out?

Mr. SCHAFFER. Again, I think that would be part of the rulemaking process to get to the ultimate rules that would make a determination.

Mr. GOODLATTE. Well, let me just add to that. I am not aware of any modern system that isn't reliant on some form of information infrastructure to operate, and if the Secretary decides for any reason that a particular system could weaken our economy, security, or safety, then he or she has unfettered authority to regulate them. Quite frankly, a lot of that seems like regulation for regulation's sake.

My question—I will address it to all of you since it is the Secretary of Homeland Security who seems to have the primary authority here. But do you think that Congress and the American people want to have their cabinet agencies turned into quasi-fiefdoms with absolute authority over the private sector? Mr. Schwartz?

Mr. SCHWARTZ. I want to take issue with this point that you raise about technical mandates. The frameworks that are being designed here are not at all technical mandates. These are performance measures. These are performance standards that industry will come together to design for themselves. That is the goal. There are no technical mandates and no technical standards within that framework whatsoever. Once industry has built those performance measures, they then create their own security plans to meet those performance measures. So they come up with what technology is needed, what standards they need to follow in order to meet those performance plans. It is purposely, specifically set up to avoid the kind of technology mandates in other bills.

Mr. GOODLATTE. Each company can have a separate standard?

Mr. SCHWARTZ. Each company could build their own—decide what technology they need to meet those performance measures. They could have completely separate technologies if they want to. It would obviously make sense——

Mr. GOODLATTE. Maybe we are engaged in semantics here, though. You call them "performance measures." I call them "technical standards."

Mr. SCHWARTZ. No. Those are two completely—coming from the National Institution for Standards and Technology, we focus on standards in terms of measurements. The goal is to come to a performance measure or a technical standard. Those are two separate things. A performance measure is to say that we need to make sure that we cut down on the number of breaches, that we act in a certain way when breaches happen, and that is tied to something that can be measured as opposed to a technical standard which is we take information in a certain way, we use a certain kind of technology, we are trying to get at a certain problem in a very specific way. We see those as two different things. And we have separated the framework that needs to be built, which is the higher performance standard framework, from the technical security plan. The security plan is built by the company not by the industry at large, not by DHS. And that is where we think the separation is.

It is exactly that reason that we think that innovation in the marketplace can grow in this space through this plan as opposed to the other bills that we have seen out there in this space that have DHS make the decisions. So we completely agree with you. DHS should not be making the decisions.

Mr. GOODLATTE. Let me give you an example, a real-time example. You have the recent Sony PlayStation attack. It could cost the company hundreds of millions of dollars. We don't know what the outcome is going to be there yet. With that type of impact on the economy, would Sony's PlayStation network fall under the "covered critical infrastructure"?

Mr. SCHAFFER. I think as conceived, there would be a process to make determinations as to what would fall under. I wouldn't, as I sit here today, think that that would have been identified as critical infrastructure, but again, those regulations haven't be written.

I do think, as a former CISO and CSO, a chief information security officer and chief security officer, for a Fortune 260 company, this kind of arrangement where the companies get to participate in identifying the risks, designing the frameworks, and then writing

their plans to meet those frameworks is flexible enough and allows for innovation. It doesn't tell a CISO, chief information security officer, what to do to solve the problem. It simply identifies the problems that need to be addressed and then gives them significant flexibility in coming up with a solution.

Mr. GOODLATTE. Well, you are asking for a lot of trust from the Congress and from the American people on this. So I guess what we will have to decide is will we want to trust the bureaucracy or are we going to try to write that much detail into legislation that clearly defines what is and what is not covered by so-called critical infrastructure.

At this time, it is my pleasure to yield to the gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman.

Let me address the circumstance under which we are here today because it is a little unusual. We have three Government witnesses here. You have submitted joint testimony, and it leads me to raise the question who is really in charge of this. I mean, most of the time, when we are doing this stuff, we have one person who is the go-to person. My understanding is that you all kind of insisted that you had to have three witnesses from the Government side. I know there are different aspects to this, but who is in charge of coming up with where you all got to? Where does the buck stop? I know it stops at the President's desk. Don't tell me that. Who is running the show?

Mr. BAKER. If I could, I will start with that, Congressman.

Mr. WATT. I don't need three answers to it. I just need one answer to it.

Mr. BAKER. At the end of the day, you are right. The President and the White House are in charge.

The proposal that we have put forward reflects a whole-of-government approach. Many aspects of the Government participate in the development of this proposal and have various "equities," if I can use that word. The Attorney General plays a certain role. The Secretary of Homeland Security plays a certain role. Different officials play different roles throughout the proposal, and what we are trying to do is bring forward something that does reflect a whole-of-government approach because the whole of government is responsible——

Mr. WATT. So every time we want some information about anything here, we are going to have to have three of you all come talk to us?

Mr. BAKER. The Department of Justice has a longstanding relationship with this Committee. If you let us know what you need, we will work to make sure we get the right people here for you.

Mr. WATT. All right.

You talked about, Mr. Baker, the Federal preemption issue. I am always a little leery of Federal preemption. We have dealt with it in a number of contexts, and generally I am leery of it because the Federal law waters down what some States have done and waters up what some States have done. So you get to some fairly vanilla middle ground.

Does your proposal provide an exemption from Federal preemption for stronger State laws?

Mr. BAKER. I think the answer is no, Mr. Chairman. the idea is that we are establishing——

Mr. WATT. Have you adopted the strongest State standard that is out there?

Mr. BAKER. The answer is I am not sure that I could tell you what all 47 statutes require, but I believe that we have looked at all the statutes and other proposals, because there have been a number of different proposals in this area both from——

Mr. WATT. Well, what is the compelling Federal interest in having a Federal standard for protecting all data, private citizen data? There are a number of things that the States have authority to do, and we are operating in a Federal system here. Why should we be preempting a State law on my personal information, breach of my personal information that is stronger than what you think the law should be?

Mr. BAKER. The compelling interest is the cybersecurity of the Nation. This is——

Mr. WATT. No. This is about my personal—this is about the personal part of my information now. I understand when it comes to national defense and homeland security, you have got a national, Federal compelling interest.

But you know, this is like consumer law, it seems to me. You know, we have gone through this debate in the financial services context. They tried to preempt every State law. The State laws in a lot of cases were a lot more robust and aggressive than the Federal law that we were trying to impose. Why would I want to do that?

Mr. BAKER. Well, again, as I said, we are trying to make this a uniform standard that makes it easier and faster that consumers find out what is going on and are aware of what has happened and makes it easier for companies to comply. So we are trying to get the balance right here.

I would say, with respect to this proposal in its entirety, we are here and we are happy to work with you.

Mr. WATT. Okay. This is the first time I am seeing this. I mean, it is a fairly new statute. But these are some of the things that I think we have got to work through.

Let me draw another parallel, if I have a little time, Mr. Chairman. You have got an immunity from liability for private industry people that seems to me to be as broad as it would be as if the Government itself were acting. This is under section 246 of this proposed legislation. And it basically says, okay, if you do what we tell you to do under section 244(e), then you are given immunity from any kind of liability. 244(e) says that it authorizes the Secretary to request and obtain the assistance of private entities that provide electronic communications or cybersecurity services in order to implement this program. That is pretty damn broad.

And it reminds me, to some extent, of the same thing that the Federal Government was asking us to do under the PATRIOT Act. The Government told you to do something. Therefore, it must be good. Therefore, you are exempt from liability. So are we setting up the same framework here?

Mr. BAKER. I will defer to——

Mr. WATT. I didn't support it there either.

I am assuming this is a legal issue.

Mr. BAKER. It is a combination, sir, and so it is liability protection, but it is if they act consistent with this subtitle, the subtitle that includes the sections you referenced. So they need to act in conformance with the law or have a good faith belief that they are doing so. Then they get liability. If they go off the reservation and do something that is not authorized, they don't get liability protection.

I will defer to Mr. Schaffer.

Mr. WATT. Okay, Mr. Schaffer. Help me.

Mr. SCHAFFER. Yes, Congressman. The provision really goes to the disclosure of any communication record or other information or assistance provided to the Department pursuant to 244(e). So what really this is trying to do is to allow the Department to work with a private sector entity that has identified an issue and wants to bring that forward for the benefit of all to protect the ecosystem.

Mr. WATT. Well, how is that different—you know, the Justice Department or somebody went out and told all the telecoms to tap anybody's phone, even though we thought it was unconstitutional to do that. And then you came back and said, well, give them immunity for doing that because we told them to do it. I mean, how is this different than that?

Mr. SCHAFFER. The statute doesn't authorize them to disclose anything that was not obtained legally. It doesn't authorize them to——

Mr. WATT. But once you tell them it is legal to obtain it, doesn't that give them complete immunity? That was the argument you were using the last time under the PATRIOT Act.

Mr. SCHAFFER. Sir, I cannot speak to what argument was made with respect to the PATRIOT Act, but I know that here the intent is to address a problem that is ongoing which is we routinely interact with a company like Sony or other companies who have had breaches, know that there is an ongoing matter of concern, and want to provide information to the Government that can be used to help that company and can be used to help a whole range of other players who are potentially at risk. In those moments, we sometimes are delayed by days or weeks in negotiation with those entities around what they can or cannot provide to the Government in that moment.

Mr. WATT. It sounds like exactly the situation you all were in. Those companies said I am not going to tap these phones because we think it is unconstitutional. You said, oh, no, it constitutional. We will give you immunity for it. So the company then is able to do something that they believe is unconstitutional just because you told them it was constitutional. And they had some ambiguous Justice Department memo that said that.

I am having trouble differentiating this. I mean, these are issues that I think we are going to have to address here. I am way over my time.

This is a little bit more than a teabag I think. This has some implications that go well beyond, I think, what has been well thought out. So I guess that is why we are here.

Mr. Chairman, I yield back. I appreciate the Chairman being generous with——

Mr. GOODLATTE. I thank the gentleman.

The gentleman from California, Mr. Issa, is recognized for 5 minutes.

Mr. ISSA. I doubt that I will be as spellbinding as the previous inquisitor, but I will agree with him.

I have got a deep concern here. Mr. Baker, why is it that this draft legislation doesn't envision the third branch of Government having a significant role? Why is it you believe that you have to essentially grant immunity without court interaction?

Mr. BAKER. Well, I guess I would have to think through—I mean, various parts of the proposal do involve the third branch of Government, for example, the critical infrastructure prohibition that——

Mr. ISSA. No, but I am talking specifically here. Look, if you go to Sony or you go to Facebook or you go to anybody, they have vast pools of information that are personal. And the Ranking Member and I share this. The tradition in this country has been you want to see it. I want you to have to make a good faith test to the third branch who stands there prepared to doubt your good intentions. It has what has kept 1984 from not happening in this country, is that you have got to go to that third branch, and they are just a little more cynical about your power grabs as a branch. We are supposed to be your balance, but without their interplay, you are going to be doing this for years to come, and all it will take is—well, you don't have two-thirds in both houses to stop a President from doing it in his Administration.

So tell me why specifically if you feel that you need to grant immunity to anybody for their cooperation, the third branch of Government should not be included?

Mr. BAKER. First of all, the provision I think you are talking about is a voluntary provision. So it only allows sharing of information in a voluntary——

Mr. ISSA. Look, I know what voluntary is. I did vote for the PATRIOT Act. I did sit on the Select Intelligence Committee. I did participate in that broad granting of immunity and pushed to get it into the bill retroactively to make it clear that we needed to put September 11th emergencies behind us.

But having said that, look, let's get back to it. You are asking for cooperation with the force of your ability to make life miserable on private sector companies behind closed doors is not a voluntary act. You can be very, very convincing. Wouldn't you agree?

Mr. BAKER. The Government can be very convincing, certainly.

What I would say is what we are trying to do and what we really tried to do in this whole proposal is get the balance right between the need to provide security, the need to allow for innovation and foster innovation, and the need to protect privacy.

Mr. ISSA. My only question to you is, as we go through this legislation, wouldn't you agree that adding in—even if it is a special court, if it is judges that are ready and quickly able to understand a comparatively complex new area of security, wouldn't you say that having that third party is a protection that this side of the dais should be interested in seeing that your side of the dais has?

Mr. BAKER. Congressman, we are happy to work with you on that. We have never said that this is a perfect proposal in all respects, and we are happy to work with you and the other Members

of Congress because, on a bipartisan basis, we want to make sure that we get this legislation right.

Mr. ISSA. Mr. Schaffer, he got the easy question. You are getting a little tougher.

The Department of Homeland Security has politicized FOIA. It has actually taken FOIA requests by the press and others, handed them over to political appointees to create an enemies list to know who was asking for what, to deny it or to spin it before it is ever released. Why is it, you think, the Department of Homeland Security is the primary place to get commercial information, not firewall to the bad guys outside our country, not terrorists within? Why do you think that you are the best place to put Facebook and Google and Microsoft and all the other providers and Sony, obviously—why is it you think you should have anything to do with it? Where do you have the standing under Homeland Security?

And by the way, why is it Mr. Schwartz wouldn't be more appropriate? Why is it that that portion isn't as much Commerce as it is this new and sometimes dysfunctional Department of Homeland Security?

Mr. SCHAFFER. Thank you, Congressman.

I think that DHS has spent a considerable amount of effort over the course of the last several years building its relationships with the private sector in this particular subject-matter area. Under the National Infrastructure Protection Plan, DHS has a major role in working with the sectors, the 18 critical infrastructure sectors, on a wide range of protection and security-related issues. With respect to cybersecurity, DHS, in particular my organization at Cyber Security and Communications, has responsibility with respect to the IT sector, the communications sector, and the Cross Sector Cybersecurity Working Group.

We work through those structures and several others to build an ongoing relationship where we actually have private sector participation on the watch floor that we use to handle cyber incidents under the National Cyber Incident Response Plan. And that relationship has been growing. We have been adding the information security analysis centers from the different sectors, participating also on the watch floor, sending representatives because they want to participate.

Mr. ISSA. Okay, I get it. I am going to be a little short only because my time has actually expired.

Mr. Schwartz, obviously, Commerce and State really have a presence overseas, and a lot of what we need to do is to reach out at all levels.

What role do you think that you should be included in a more robust way than you are under this proposal?

Mr. SCHWARTZ. Well, I think this proposal does lay out ways that NIST and Commerce can be deeply involved, but it involves the private sector bringing us in for those cases. So, for example, in the critical infrastructure plans piece, if they want to invite NIST to help work with them to plan international standards to help them build the framework so it can lead to security plans and figure out how that can work better together and they want NIST to participate in that, the private sector can bring us in to do so. Obviously,

we have limited resources to be able to get involved in every different critical infrastructure area, but that is one place——

Mr. ISSA. So you currently see you are going to be reactive, not proactive because of the nature of it. Wouldn't it be better for you to have a mandate to be proactive?

Mr. SCHWARTZ. There are some places working with the Federal Government agencies, for example, where we are setting standards for the Federal Government, where we are being very proactive. And some of those are then ending being used by the private sector. So in terms of the question of protecting the critical infrastructure as it relates to the private sector, we need to be brought in for that. For the Federal Government, we are much more proactive. And I think we want it that way. We don't want to be setting technical standards for the private sector, as I said to the Chairman earlier. I think that is very important that we are working with the private sector cooperatively and we are setting standards that can work for Government, and then we can figure out how those can be used together.

Mr. ISSA. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. GOODLATTE. I thank the gentleman.

The Chair recognizes the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman.

Mr. Schaffer, the notice would have to be given to an entity of the Department of Homeland Security. That is a national standard requirement for reporting breaches of private consumer data. What entity of the Department of Homeland Security?

Mr. SCHAFFER. I think, as we are currently constructed, it is the NCIC and U.S. CERT entity. I think that the drafting recognizes that names of entities can change over time, but the notion is that that portion of my organization at Cyber Security and Communications would be where those central reports would flow.

Mr. CONYERS. So everybody has got to come back and read this transcript to find out what the answer to my question is.

Mr. SCHAFFER. I apologize, sir. The United States Computer Emergency Response Team is part of the Cyber Security and Communications organization, and there is a watch floor called the National Cyber Security and Communications Integration Center that works with U.S. CERT to be a collection point for information aggregation and dissemination.

Mr. CONYERS. So we just go to some entity and that is what it is. So now we know.

All right. Who is going to have primary responsibility to investigate criminal violations as between the FBI and the Secret Service?

Mr. BAKER. As it is today, it is a variety—the two of them work it out. They coordinate their activities to determine who is going to investigate a particular offense. They have overlapping jurisdiction. They have to coordinate their activities, and so that is how it is done with those agencies. It is common to do that with a variety of different law enforcement agencies that exist in the Federal Government.

Mr. CONYERS. Well, they have enough differences of opinion often enough as it is.

Mr. BAKER. They may have differences of opinion. At the end of the day, they don't get to go to court unless they come through the Department of Justice. The Department of Justice is in control of what cases get indicted and what cases are brought forward and how appeals are handled and so on and so forth. So at the end of the day, it is the Attorney General.

Mr. CONYERS. Thanks, Mr. Chairman.

Mr. GOODLATTE. I thank the gentleman.

And the Chair now recognizes the gentleman from Arizona, Mr. Quayle.

Mr. QUAYLE. Thank you, Mr. Chairman, and thanks to all the witnesses for being here.

One thing I want to know—it is for all of you and whoever best can answer this just pipe in. Can you explain exactly how you plan to address some of the duplicative regulation work that might be happening here? Because NIST has historically been the lead agency in setting standards, especially working with industry to create those standards. But the Administration's proposal seems to shift that responsibility to DHS.

For example, will DHS first assess the cybersecurity requirements of the various Federal agencies to determine if they are adequate before creating their own regulations, or do you intend that DHS just creates their own regulations and then waits for the request from various agencies for exceptions?

Mr. SCHWARTZ. Let me just briefly talk about NIST's role because I think there is a misunderstanding there about what NIST's role currently is. NIST today sets the standards for the Federal Government. Then OMB takes that and approves them for the agencies.

Under this proposal—and there has recently been a memo that also passed some of that authority to DHS. So this would codify the ways that things are actually currently being run, which is that NIST would still write the standards. In fact, the Secretary of Commerce publishes those standards. It is very clearly in the proposal. Then DHS can draw on those to decide what the agencies should do specifically.

So NIST is still writing the standards the way that we have and we will continue to write the standards in that way and, in fact, gain slightly more independence in that because OMB has traditionally just passed on exactly what we have said to the other agencies. This will allow DHS to tailor better to different agencies and hopefully create better technical standards that can be tied to performance standards as well so that we can react better more quickly over time inside of the Federal Government.

Mr. QUAYLE. But so then is DHS then going to take the various standards that NIST comes up with and then implement them through the other various Federal agency, or is the Federal agency going to be able to use NIST standards to create their own cybersecurity framework within that agency and then have to get approval from DHS?

Mr. SCHAFFER. As Mr. Schwartz said, this really codifies the way things are operating now through delegations of authority. So NIST would continue to draft the standards. DHS would take those standards and would be applying them to the Departments and

agencies. If Departments and agencies had specific issues that needed to be addressed in some special way—the standards are not written for each individual agency, they are written holistically—then we would be in a position to work with an agency and come up with a set of requirements that made sense specifically for the set of threats or risks. But ideally we would be working starting from the NIST standards just as we are today, and as Mr. Schwartz said, that was being done by OMB recently delegated through a memorandum to DHS. But the statute would just codify that oversight authority moving to DHS.

Mr. QUAYLE. And, Mr. Schwartz, when you are talking about the standards that are being developed by NIST, that kind of does conjure up a very static procedural way that we are not going to be able to have the flexibility to respond to various cyber threats which evolve very quickly in the future. How is NIST going to develop those standards and do them in a way that allows for the flexibility to have best practices from various areas to come in and make sure that, instead of just being reactive, we are being proactive to make sure that we are still using the best standards to address cybersecurity threats?

Mr. SCHWARTZ. One of the problems we have today under FISMA is that the focus has been on trying to cover all of the different controls that NIST puts out, so the IG, the Inspector General, has said you have to make sure that you cover all of these controls rather than saying we need to focus the controls that work best for each agency, which is what NIST really says in our guidance on the subject. So this structure helps to get that point across better, that we are really aiming at performance here and not at you have to follow every single standard that NIST puts out.

As NIST puts these out, we do think that we have flexibility and we spend a lot of time with some more technical standards. Encryption is a good example of that, which we try to think very far ahead in trying to make sure that things are done, and the world depends on the NIST encryption standards for that reason because it is so thought out, et cetera. There are others that we try to act much more quickly, try to be reactive, et cetera, and get things out very quickly. So we try to have that kind of flexibility so we can do both.

But we need the independence also of not having to answer every agency question that comes in on every topic. We need someone to be able to do that. We work with the agencies as clients, et cetera, and work with them on the standards, but there is a different piece of it in terms of performance and getting the performance measures out. It is good to have another body do that. OMB was doing that role before. Now that is moving more to DHS.

Mr. QUAYLE. Thank you very much.

I yield back.

Mr. GOODLATTE. I thank the gentleman.

The gentlewoman from Florida, Ms. Adams, is recognized for 5 minutes.

Ms. ADAMS. Thank you, Mr. Chair.

Earlier I heard you, Mr. Schwartz, say "performance measures." Can you give me your definition for performance measures?

Mr. SCHWARTZ. What we are aiming at is trying to figure out exactly how to improve the actual way that the Internet is protected so that we can come up with measures that show when we have been successful in protecting cybersecurity as opposed to "technical standard," which is to say that you must follow a certain set of controls in order to come up and make sure that you are interoperable with other types of controls.

Ms. ADAMS. So that is your explanation of performance measure.

Mr. SCHWARTZ. Again, performance measure is something that can be measured that shows that you are continually improving the cybersecurity as we know it, that we can show continued positive performance over time.

Ms. ADAMS. Well, I have to tell you that your description kind of concerns me because you had to grapple at what it was. So it concerns me when an agency is going to decide what the performance standards are when they are still grappling with what are the performance standards, how do you define performance standards.

Mr. SCHWARTZ. Again, I am not the technical person that is going and writing these technical standards, and I am not the person that is writing the performance standards. What a performance standard will be will be a particular number or a particular set of—particular targets.

Ms. ADAMS. So that is not static.

Mr. SCHWARTZ. It is not static, exactly. It is something that is not static. It is something that can change over time, something that can be revisited, whereas a technical standard is something that is written, people need to be able to follow it and be able to interoperate.

Ms. ADAMS. And following along what—Mr. Watt I believe was the one that brought it up on the Federal preemption with Mr. Baker. You said that you had not reviewed all 47—that they had been reviewed, but you had not reviewed them. So you don't know if the Federal preemption would preempt a State that actually might have a better system than what the Federal Government would come up with. Is that correct?

Mr. BAKER. That is correct.

Ms. ADAMS. So you still advocate for Federal preemption even though you could actually do more harm than good?

Mr. BAKER. Well, our folks have looked at it carefully and we believe that this is the right balance. If there are State standards that Members of Congress feel should be included in the Federal legislation, we are happy to work with you on that. We have tried to get the balance right. If you think we should add things, we are happy to work with you and look forward to that because we want to make sure that——

Ms. ADAMS. Well, I am happy to hear that agencies want to work with us on legislation that we would be drafting. That is a good thing. I would hate to think that you would think you could draft the legislation.

Let's see. Mr. Schaffer, I believe. You are from DHS? Do you believe that there should be limits to the power that the Secretary of Homeland Security can exert on private industry?

Mr. SCHAFFER. I am sorry. I missed the last phrase.

Ms. ADAMS. Do you believe that there should be limits to the power that the Secretary of Homeland Security can exert on private industry?

Mr. SCHAFFER. I am sorry, ma'am. I believe——

Ms. ADAMS. That is a yes or a no?

Mr. SCHAFFER. Yes, and I think they are in the statute.

Ms. ADAMS. Would the Administration's plan give the Secretary unfettered authority over any business?

Mr. SCHAFFER. No, it certainly wouldn't give unfettered authority.

Ms. ADAMS. Maximum authority?

What large industries would be excluded?

Mr. SCHAFFER. Ma'am, the way the statute is configured—and I assume that we are talking about the critical infrastructure portion of the statute because other portions have a different scope.

Ms. ADAMS. Are there any that have been excluded so far?

Mr. SCHAFFER. I certainly don't think that every large enterprise would be part of critical infrastructure under this construct.

Ms. ADAMS. How about under cybersecurity as a whole that would be monitored under this?

Mr. SCHAFFER. Certainly the statute is designed to improve cybersecurity across the entire ecosystem, but the critical infrastructure piece is, indeed, intended to be focused on critical infrastructure, those infrastructures which, if disrupted through a cyber attack, would have cascading and devastating effects across a significant portion of our day-to-day lives.

Ms. ADAMS. Mr. Baker, do you know any that would be excluded?

Mr. BAKER. I am sorry.

Ms. ADAMS. Any industries that would be excluded outside the critical infrastructure? Large corporations.

Mr. BAKER. Categories of industries. I mean, I guess it depends on the facts and circumstances and how they interrelate, but I think I——

Ms. ADAMS. How would you define that? Would that be clearly defined in what you were doing?

Mr. BAKER. In the proposal that I was talking about earlier on the critical infrastructure, we have got a fairly specific——

Ms. ADAMS. I am sorry, Mr. Chair. I guess I have overrun my time.

But I am just curious. If you are outside the critical infrastructure, you are on the cybersecurity issue, is there any of that that falls into the exclusion?

Mr. BAKER. Any that would fall into the exclusion in terms of the—well, with respect to the proposal I was referring to, we couldn't use it if it didn't meet the test that was set forth in the statute, and that would be determined at the end of the day by a court. We would have to make the case to the court that it was part of the——

Ms. ADAMS. You think it might end up in court.

Mr. BAKER. Well, this one, the one I am referring to, absolutely would, yes, because it would be a criminal offense and we would have to show that it was vital to the country.

Ms. ADAMS. I was actually talking about the statute if we were to pass it.

Mr. BAKER. The statute what? I am sorry.

Ms. ADAMS. The law, if we were to pass it. I thought you meant you thought it would be in court.

Mr. BAKER. I am sorry. I couldn't hear, Congresswoman. I am sorry.

Mr. GOODLATTE. I thank the gentlewoman.

And the gentleman from Pennsylvania, Mr. Marino, is recognized for 5 minutes. The gentleman has no questions.

We will thank our panel then. This has been very interesting, and I think it is just the beginning of a lot of discussion about the Administration's proposal and potential legislation that I and others are working on here in the Congress. So we very much appreciate your contribution, and we will thank all of you and excuse you and move to the second panel.

We will now move to our second distinguished panel of witnesses today, and as I advised earlier, each of the witnesses' written statements will be entered into the record in its entirety. And I ask that each witness summarize his or her testimony in 5 minutes or less, and to help stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, that is it.

Before I introduce our witnesses, I would like them to stand and be sworn, and we would ask you to do that at this time. It is the custom of the Committee to swear in our witnesses.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much.

Our first witness is Mr. Robert Holleyman. Mr. Holleyman serves as the President and CEO of the Business Software Alliance. He has headed BSA since 1990, expanding their operations to more than 80 countries and launched 13 foreign offices, in addition to their D.C. headquarters. Mr. Holleyman has been named one of the 50 most influential people in the intellectual property world by the international magazine, Managing IP. He was also named by the Washington Post as one of the key players in the U.S. Government's cybersecurity efforts for his work on behalf of industry on national cybersecurity policy.

Before joining BSA, Mr. Holleyman served as counsel in the U.S. Senate and was an attorney with a leading law firm in Houston, Texas.

He earned his bachelor of arts degree at Trinity University in San Antonio, Texas and his juris doctor from Louisiana State University Law Center in Baton Rouge. He also completed the executive management program at the Stanford Graduate School of Business.

Our second witness is Mr. Leigh Williams. Mr. Williams serves as BITS President for the Financial Services Roundtable. Since 2007, Leigh Williams has served as President of BITS, the technology policy division of The Financial Services Roundtable, focusing on improving operational practices and public policy in the financial sector. Previously Mr. Williams was a senior fellow at Harvard's Kennedy School of Government researching public and private sector collaboration in the governance of privacy and security.

Mr. Williams worked for many years at Fidelity Investments in various risk, security, privacy, and policy roles, including chief risk officer, chief privacy officer, and senior vice president for public policy.

Mr. Williams earned a bachelor of arts in economics from Rice University and a master of public and private management from Yale University where he currently serves as the Yale School of Management Alumni Association President.

Our third witness is Ms. Leslie Harris. Ms. Harris serves as the President and CEO of the Center for Democracy and Technology. Ms. Harris is responsible for the overall direction of the organization and serves as its chief strategist and spokesperson. Ms. Harris has worked extensively in policy issues related to civil liberties, new technologies, cybersecurity, and global Internet freedom. In 2009, she was named one of Washington's "tech titans" by Washingtonian Magazine.

Prior to joining CDT, Ms. Harris founded Leslie Harris and Associates, a public policy firm. She has also worked for the People for the American Way and the American Civil Liberties Union.

Ms. Harris received her B.A. from the University of North Carolina at Chapel Hill and her law degree from the Georgetown University Law Center.

I want to welcome all of you and we will begin with Mr. Holleyman.

TESTIMONY OF ROBERT W. HOLLEYMAN, II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE (BSA)

Mr. HOLLEYMAN. Thank you. Chairman Goodlatte, Ranking Member Watt, BSA appreciates the opportunity to work with this Committee on a variety of challenges that we face in the area of cyberspace. These include the continuing problem of software piracy and threats to cybersecurity. Indeed, the two issues are connected because pirated software, which cost our industry nearly $60 billion last year, is increasingly used to distribute malicious computer code, and this puts companies, governments, and consumers at risk.

Today I would like to address three issues: first, the evolving nature of security threats; second, the link between piracy and the spread of those threats; and third, specific actions this Committee should take to address these problems.

Just 10 years ago, the primary threats to security online were hackers and vandals, and they primarily chased notoriety and the opportunity to take down systems through denial-of-service attacks against entities like eBay and CNN.

But the stakes are now much higher. Organized criminals have entered this arena and they are using the Internet to distribute malware so that they can make big money. And today's scams build off both fears and social trends, and they take advantage of worms, viruses, adware, links to fake websites, and other fraudulent activity, and they steal valuable data from consumers and enterprises. It has been estimated that for U.S. businesses alone, the costs of this are approximately $45 billion annually.

The link to software piracy is also evolving. The research firm IDC estimates that fully one-third of illegally installed software

contains some form of malware, and organizations using pirated software have a 73 percent greater chance of serious security problems than companies that use licensed software.

Before turning to specific legislative recommendations, I would like to note, and importantly for this Subcommittee and Committee, that the U.S. Government does not yet have in place a policy to require Federal contractors to use licensed software, even though Federal agencies must. And, indeed, I find it astonishing, given the security threats associated with illegal software, that this action has not been taken. The Administration is now considering an executive order that would require Federal contractors to use licensed technologies, and I urge this Committee to express its support for that order and push the Administration to act in this area.

We believe this Committee can also bolster America's cybersecurity in at least three additional ways.

First, by strengthening the hand of law enforcement and prosecutors. As cyber criminals adapt, so must our cyber crime laws, and BSA supports legislation to strengthen penalties and expand the scope of offenses. We need new causes of action that toughen the hand of prosecutors while, at the same time, preventing opportunistic private litigation.

Second, we need clear, uniform Federal data protection and data breach rules. Today more than 40 States have enacted such laws. This patchwork is confusing for consumers and inefficient for businesses. The Federal Government should require notification of breaches that pose a genuine risk of harm. It should preempt State laws, and it should prevent excessive notification which can overwhelm and confuse consumers. Importantly, notification should not be required when the stolen data is worthless to the thief because it has been rendered unusable through deployment of security technologies such as encryption.

And finally, the law should provide specific incentives for sharing information about cyber threats with Government agencies. Companies should be able to share records and other information with DHS about the specific nature of the threat without the risk that sharing that information will lead to suits against the company. Similarly, critical infrastructure companies that comply with the security requirements of DHS or act to mitigate risks identified by DHS should also be protected from liability.

Lastly, Mr. Chairman, Mr. Ranking Member, Mr. Quayle, this Committee is looking at the consequences of cybersecurity as they affect the Nation's economy. The economic consequences of this are greater for this Nation than any other because of the way in which we deploy this technology throughout our society. And by acting to deter cyber threats and to take more actions, we can believe that the economy will be healthier by deploying new resources to creating new jobs and overall strengthening economic security.

So I look forward to working with this Committee as always on these important issues. Thank you.

[The prepared statement of Mr. Holleyman follows:]

U.S. House of Representatives

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition and the Internet

Hearing on "Cybersecurity: Innovative Solutions to Challenging Problems"

Testimony of Robert W. Holleyman II
President & CEO, Business Software Alliance

Wednesday May 25, 2011

Chairman Goodlatte, Chairman Sensenbrenner, Ranking Member Watt, Ranking Member Scott, thank you for holding this hearing today and for inviting me to testify. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance (BSA.) BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world.[1]

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies and considerable cost savings and it will continue to produce immense benefits to our global society.

However, this revolution has brought with it a number of risks. We all face a variety of online threats, which can undermine trust in the digital environment – the single greatest platform for commerce and sharing information.

BSA has greatly appreciated the opportunity to work with the members of this Committee over the years to address some of the challenges we face in cyberspace, including the continuing problem of software piracy and the threats to cybersecurity. Indeed, the two issues are connected: the use of illegal software is often an entry point for computer malware that jeopardize not only the security of that particular computer but the security of the networks to which that computer is connected.

1. The Size and Nature of the Threats

The gravity and nature of the threats to cybersecurity are significant. These threats fall into four categories according to their motives:

1. Cybercrime—For several years now, cybercrime has been overwhelmingly fueled by profit, employing sophisticated technologies capable of highly targeted attacks that increasingly emanate from organized crime.
2. Espionage targeting corporations—Cyber attacks against the computers, servers and networks on which companies depend have reached unprecedented levels of sophistication, with the aim of committing extortion or stealing intellectual property and other trade secrets for the benefit of competitors;
3. Espionage targeting governments—Governments have become as reliant on information technology as corporations have; as a result, advanced persistent threats that penetrate government computers, servers and networks can produce significant intelligence;

[1] The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Compuware, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, and The MathWorks.

4. Cyber warfare—The dependence of a Nation on cyber resources can be exploited by another to electronically disable its critical infrastructure, essential governmental services and military capabilities.[2]

Some of the major attack trends that Symantec detailed in its latest Internet Security Threat Report include:[3]

- Targeted attacks—attackers increasingly identify specific targets and develop sophisticated plans for compromising their computers. They have learned "that the easiest vulnerability to exploit is our trust of friends and colleagues."
- Social networking—linked to the first trend is the exploitation of online social networks which "provide rich research for tailoring an attack" allowing hackers to "learn our interests, gain our trust, and convincingly masquerade as friends."
- Stealth—Once inside an organization, a targeted attack attempts to avoid detection until its objective is met. Exploiting zero-day vulnerabilities[4] and using rootkits[5] are two effective ways of evading detection.
- Attack kits—the sophisticated stealth attacks mentioned above are not exclusive to a few elite cyber attackers. They are packaged and traded as easy to use attack kits in a vast underground economy.

Another way to gauge the cyber threats we face is to look at a simple and compelling number: McAfee reports that in 2010, they detected an average of 60,000 new pieces of malware – i.e. malicious software – *each day*.[6]

This testimony addresses several aspects of our collective response to this challenge, including the role that Congress needs to play. Recently, the Administration made a number of legislative proposals, many of which we could support with appropriate modifications. It is clear that the Judiciary Committee has an essential role to play in strengthening the hand of law enforcement and prosecutors as they battle cybercriminals, and in providing appropriate incentives for private sector entities to further improve their cybersecurity and to share information that allows us to improve our collective cybersecurity posture.

2. The technology industry's response to the challenge

Protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem by itself – and no individual or group is without responsibility for playing a part in cybersecurity. The technology industry, consumers, businesses and governments must all take steps to secure their own systems and to collaborate with each other to define and implement comprehensive cybersecurity policies and technologies.

---

[2] See http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/05/03/the-cyber-threat-deconstructing-the-problem-to-promote-comprehensive-dialogue-and-action.aspx

[3] Symantec Corp., Internet Security Threat Report, Vol. 16: http://www.symantec.com/business/threatreport/index.jsp

[4] Zero-day vulnerabilities are previously unknown, and therefore still unpatched, software vulnerabilities.

[5] A rootkit is malicious software that provides an attacker with privileged and undetected access to a computer.

[6] "A Good Decade for Cybercrime – McAfee's Look Back at Ten Years of Cybercrime", http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf

The technology industry's responsibilities in the face of cybersecurity challenges are fourfold.

First, each and every day our members focus on the trustworthiness of the information technology products, systems and services. Since governments, critical infrastructure providers, businesses and consumers worldwide depend upon these technologies for their daily operations and business processes, our members have undertaken significant efforts to reduce vulnerabilities, improve resistance to attack and protect the integrity of the technologies they provide.

Users can expose themselves to cybersecurity risks when they use counterfeit or unlicensed technologies. Users of counterfeit hardware or software have no assurance of their trustworthiness, and in many cases intentional vulnerabilities – i.e. malware –are found in counterfeits.[7] In fact, most PC users seem to understand this risk: in a survey of 15,000 PC users in 32 countries, conducted by the respected research firm Ipsos Public Affairs as part of the 2010 BSA Global Software Piracy Study, eighty-one percent of respondents say that fully licensed software is better than pirated software in providing protection against computer viruses or hackers. Eighty-six percent of respondents also say that protection against computer viruses or hackers is an important factor in determining which software to use.[8] That is why our industry consistently advocates that technology users – whether consumers, businesses or government agencies – purchase only from authorized dealers and resellers and use commercial anti-piracy and anti-counterfeiting technologies and processes.

Indeed, in order to better protect themselves, BSA has advocated that organizations adopt Software Asset Management (SAM.) SAM is the people, processes and technology necessary for the effective management, control and protection of the software assets within an organization, from acquisition to retirement. SAM enables organizations of all sizes to realize the full potential of, and value from, their software investments, such as: controlling license compliance, ensuring ongoing software cost-efficiency, and meeting IT governance requirements. The International Organization for Standardization (ISO) developed the ISO/IEC 19770-1 SAM standard to enable organizations to demonstrate that they are managing their software assets to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. BSA developed an online course and certification, SAM Advantage, to allow IT professionals to learn how to effectively manage software assets in their organization.[9]

Second, our members work diligently to develop security technologies to defend against evolving threats. Users of technology rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

Third, our members are leaders in educating and raising public awareness of cyber risks and how users can protect themselves. Many of our members have developed their own substantial programs to convey these messages, and many offer free security checkup tools. In addition, several BSA members

---

[7] See for example the 2006 IDC White Paper on "The Risks of Obtaining and Using Pirated Software." It showed that 25% of the Web sites that were reviewed for the study that offered counterfeit product keys, pirated software, key generators or "crack" tools attempted to install either malicious or potentially unwanted software. It also showed that 11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from peer-to-peer networks contained either malicious or potentially unwanted software.

[8] http://portal.bsa.org/globalpiracy2010/

[9] More information about SAM is available at http://samadvantage.bsa.org/

play a leading role in the National Cyber Security Alliance (NCSA),[10] a non-profit organization supported by public and private sector partners. NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets. In 2010, NCSA and the Anti-Phishing Working Group (APWG),[11] launched the "Stop | Think | Connect" campaign, the first-ever coordinated message to help all digital citizens stay safer and more secure online. The hope is that "Stop | Think | Connect" will achieve for online safety awareness what "Smokey Bear" did for forest fire safety and "Click It or Ticket" did for seatbelt safety.[12]

Finally, our members partner with the government to develop and implement policy, share information about threats, and respond to incidents. Given the complexity and interconnected nature of information systems and networks, as well as an ever-evolving and sophisticated threat environment, no one organization or entity can address U.S. national cybersecurity alone. Industry entities work together, government entities harmonize their approaches to protecting critical infrastructure, and government and industry work together to address common concerns and build collaborative solutions. The public-private partnership on critical infrastructure protection and cybersecurity, currently organized under the framework of the National Infrastructure Protection Plan (NIPP), is sound, widely accepted, and one in which both government and industry are heavily invested.

3. The Judiciary Committee's role in improving cybersecurity

Cybersecurity is a major challenge. While industry takes its responsibilities seriously and devotes considerable time, energy and resources to the fight, we believe legislation in several areas within the Judiciary Committee's jurisdiction would be extremely helpful.

We believe that this Committee has the opportunity to improve cybersecurity in a way that strengthens the hand of law enforcement and prosecutors, provides incentives to companies to improve cybersecurity, rewards industry leadership and furthers collaboration between the public and private sectors. We make five recommendations towards that goal.

a. Criminal laws

For several years now, cybercrime has been overwhelmingly fueled by profit, employing sophisticated technologies capable of highly personalized attacks increasingly emanating from organized crime. Thus BSA has long championed the need to equip investigators and prosecutors with the tools they need to effectively fight cybercriminals.

We thank this Committee for the leading role it played in securing the enactment in 2008 of the Identity Theft Enforcement and Restitution Act. This law, which was the most significant modernization of the Computer Fraud and Abuse Act (18 USC 1030) in a decade, resulted from remarkable bipartisan

[10] http://www.staysafeonline.org
[11] http://www.apwg.org
[12] http://www.stopthinkconnect.org/

cooperation within and among this Committee, the Senate Judiciary Committee and the U.S. Department of Justice.

We cannot stop there. As cybercriminals continue to adapt, so must our laws. BSA broadly supports the Administration's law enforcement legislative proposals, which strengthen penalties and expand the scope of offenses.

We would like to recommend however an important modification to the Administration's law enforcement proposals, to avoid unwarranted treble damages.

Part 2 of the bill adds cybercrime to the list of offenses that can be prosecuted under the Racketeering Influenced and Corrupt Organizations Act (RICO, 18 USC 1961(1).) Cybercrime has often become an organized criminal activity. We therefore believe it is appropriate to allow *criminal prosecution* of cybercrime as an organized crime, with the effective tools of the RICO statute. However, the proposal does not consider the risk that this creates for legitimate businesses on the *civil liability* side. Listing an offense in 18 USC 1961 opens the way for a civil plaintiff to seek treble damages, as well as the cost of the lawsuit including a reasonable attorney's fee, under 18 USC 1964(c). While legitimate businesses do not participate in organized crime, any attorney could create a very effective threat just by filing for discovery, seeking treble damages and exposing a company to the considerable reputational damage of being branded an "organized criminal enterprise." This would often be sufficient for legitimate businesses to agree to an out-of-court settlement, however undeserved by the plaintiff.

We therefore urge that Congress follow the reasonable and legitimate precedent it has already set with regard to securities fraud, by excluding cybercrime from 18 USC 1964(c). We believe this would have no effect on prosecutorial authority against cybercrime under RICO.

b. Data security and data breach notification

BSA supports efforts to enact a federal law requiring that organizations secure the sensitive personal information that they hold, and notify individuals when that security has been breached.

Consumers' trust in the security and confidentiality of their sensitive personal data is eroding. Over the past several years, the number of significant database security breaches has increased dramatically. The stakes are high and getting higher all the time. According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 533 million records containing sensitive personal information since 2005.[13] For example recent intrusions into Sony's PlayStation Network led to the theft of sensitive personal information related to 77 million accounts.

BSA believes that federal legislation that requires organizations to secure the sensitive personal information that they hold, and notify individuals when that security has been breached can effectively help restore consumers' trust. Such data breach notification legislation should be based on the following criteria.

[13] http://www.privacyrights.org/data-breach

Establish a uniform national standard that preempts state laws

The National Conference of State Legislatures (NCSL) indicated that, as of October 2010, forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws.[14] This patchwork of state laws has created a compliance nightmare for businesses. Importantly, it can also create confusion for consumers who receive notices from a multiplicity of sources. Federal legislation establishing a uniform national framework would therefore benefit businesses and consumers alike. Section 109 of the Administration's data breach notification legislative proposal also would preempt state laws, but we recommend that legislation preempt state requirements that breach notices include information regarding victim protection assistance provided by that State.

Prevent excessive notification

Not all breaches are of equal importance. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Currently, most state data breach laws require notification in all instances, even when no risk results from the breach. Over notification is likely to numb consumers, who will then fail to take appropriate action when they are truly at risk. A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm.

Section 101(a) of the Administration's data breach notification legislative proposal requires that the breach creates a risk of harm or fraud. While this is a step in the right direction, we recommend that the threshold be raised from "*reasonable risk*" to "*significant risk,*" to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable

BSA believes that data security can be much enhanced, without a significant and difficult-to-enforce regulatory system, simply by using a market-based incentive for the adoption of strong data security measures. This can be done through an exception to the proposed obligation to notify security breaches in cases where the data is protected, so that even if it "*gets out*" the information cannot be used.

BSA believes this can be achieved if the measure in question satisfies two conditions:

1. It must render data unusable, unreadable, or indecipherable to any party that gains unauthorized access.
2. It must also be widely accepted as an effective industry practice or an industry standard. Examples of such measures include, but are not limited to, encryption, redaction, or access controls.

Under these two conditions, the data that has been accessed cannot actually be used to defraud or inflict harm on data subjects. A breach would not pose a risk to the data subjects. Therefore, the apparent breach should not require notification.

---

[14] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

In this regard, the Administration's proposal got it right. Section 102(b)(1)(A) of the Administration's data breach notification legislative proposal provides such a market-based incentive for the adoption of strong data security measures. We are particularly supportive of the fact that this incentive is technology neutral, in other words that it does not favor any specific technology. This ensures that innovators will continue to develop new techniques and methods, and organizations will continue to adopt them, without feeling that legislation has favored one type of measure over another. It is also demanding enough to provide a high degree of protection for consumers, today and tomorrow.

Include data security safeguards

Requiring breach notification is fair to consumers who need to know they are at risk, but we believe we should do more to prevent breaches from happening in the first place. We support the inclusion in federal legislation of provisions requiring organizations that hold sensitive personal information to establish and implement reasonable and appropriate data security policies and procedures. Such a requirement should be flexible, by providing that these policies and procedures should take into account the size, scope and nature of the organization's activities and the cost of implementing safeguards. These requirements should also avoid prescribing the use of specific security technologies or methods, and rather ensure that the organization selects those technologies and methods that are most appropriate to their circumstances and risk profile.

Such preventative security requirements have been included in every bill discussed in Congress in the last several years.

Appropriate enforcement

Whether this enforcement authority rests with the U.S. Attorney General or the Federal Trade Commission (as the Administration proposes) what is needed is vigorous action to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We also support the inclusion, in section 108 of the Administration's proposal, of state Attorneys General (AGs) as enforcers, when federal authorities have not acted. The FTC has limited resources and as a result appropriately focuses on large or precedent-setting cases, while state AGs can supplement the FTC in other cases worthy of enforcement.

We believe however that state AGs should be required to bring their civil actions under the bill in federal, rather than state, court. Federal jurisdiction would ensure that this federal legislation is applied consistently throughout the country.

BSA believes it is also important to prevent excessive litigation. Allowing private lawsuits as a result of the occurrence of a data breach would create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits. Section 108(f) of the Administration proposal also clarifies that their bill does not establish a private cause of action.

c. Incentives for information sharing

Sharing information about threats and vulnerabilities and their consequences greatly contributes to more effective collective risk mitigation, and thus improves cybersecurity.

Many private sector companies, in particular in the information technology sector, have invested important resources into information sharing, in particular by dedicating personnel to gathering and analyzing the data and to participating in collaborative information sharing mechanisms such as the IT Information Sharing and Analysis Center (IT ISAC.)

We believe legislation can make an important contribution to improving information sharing, by removing some of the legal barriers that have been identified. In this respect, the Administration has made two useful proposals.

First, section 245 of the Administration's legislative proposal on the cybersecurity authorities of the Department of Homeland Security (DHS) authorizes companies that lawfully intercept, acquire, or otherwise obtain or possess any communication, record or other information to disclose that information to DHS for the purpose of protecting the cybersecurity of an information system. This is appropriate because current law authorizes the collection, use, and disclosure of information for self-defense purposes, but does not provide explicit authority to do the same for the defense of others. We note that this proposal contains useful privacy safeguards, such as requiring that reasonable efforts be undertaken to remove information that can be used to identify specific persons unrelated to the cybersecurity threat before any disclosure, and that further disclosures and use of the information that was shared be subject to a number of restrictions.

Second, section 246 of the Administration's legislative proposal on the cybersecurity authorities of DHS prohibits a civil or criminal cause of action against a company that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record or other information and discloses that information to DHS for the purpose of protecting the cybersecurity of an information system. This is needed because the fear of liability has long been known to inhibit information sharing.

We would encourage you to consider an additional market-based incentive for sharing information. We believe it would be appropriate to create a safe harbor from liability, so that information that is shared about an incident cannot be used to seek damages against the company that experienced the incident. Again, we believe that, with the right privacy protections in place, encouraging companies to share information about threats and vulnerabilities without fear of exposing themselves to liability can significantly contribute to improved cybersecurity.

d. Incentives for the cybersecurity of critical infrastructure

We believe this Committee can make an important contribution to cybersecurity by providing liability protection to companies identified as critical infrastructure.

These incentives would be provided to companies operating systems or assets designated as critical infrastructure when these companies are complying with the cybersecurity requirements of DHS, or when they are taking reasonable and appropriate steps to mitigate risks identified by DHS but for which DHS has not approved best practices. Under such conditions, these companies should be protected from related liability, whether for direct, indirect, economic, non-economic or punitive damages.

Other Committees have been, and we hope will remain, interested in the issue of liability protection as it is part of the regulatory framework they have proposed for critical infrastructure. We have other recommendations, which we highlight in the last section of this testimony, about the rest of that

regulatory framework, and we need to make sure they are addressed before that framework is adopted by Congress.

However, we bring this specific aspect of the proposed regulatory framework to the attention of the Judiciary Committee, separately from the rest of that framework, for three reasons. First, because issues of liability protection are relevant to the jurisdiction of the Judiciary Committee. Second, because providing incentives in the form of liability protection strengthens the public-private partnership model that has been successful in improving our Nation's cybersecurity. And third, because this approach will not strain the organizational or budgetary resources of the government, which we recognize is an important consideration in the current fiscal climate.

e. Require that federal contractors use licensed software

Finally, the Obama Administration is considering issuing an Executive Order to require Federal contractors to use licensed technologies, including software. This follows an Executive Order issued some ten years ago requiring government agencies to use licensed software.

We urge this Committee to express its support for this new Executive Order. Using licensed software is not only required by our copyright and patent laws, but as noted above is essential to maintaining security and avoiding the malware that is often bundled with pirated software.

4. Congressional action should also be guided by the following objectives

In addition to the above recommendations, which we think are of most relevance to the Judiciary Committee, other Committees and the Administration have signaled that they want to address a host of other cybersecurity issues. In fact, their proposals contain a number of very useful provisions, although some important improvements are needed. We would like to highlight a few significant considerations.

a. Reforming the Federal Information Security Management Act

Federal agencies are under regular and persistent cyber threats from criminals and hostile nations. The enactment in 2002 of the Federal Information Security Management Act (FISMA) was an important milestone, but its implementation has not improved information security as much as it was hoped. Agencies can comply with FISMA and yet still have significant gaps in their actual security.

We will continue to work with the Administration, the House of Representatives and the Senate towards enactment of effective FISMA reform and to providing the corresponding funding, to ensure that agencies have the authority, resources and obligation to identify and mitigate the cyber risks they actually face.

b. The scope of critical infrastructure

The security of critical infrastructure has been a major focus of cybersecurity legislation. The Administration's legislative proposal and the comprehensive bill currently being developed in the Senate both create a regulatory framework for critical infrastructure.

The scope of what is critical infrastructure is particularly important. We must define "critical infrastructure" in a manner that is not excessively broad, to avoid overstretching the resources of DHS and imposing a potentially cumbersome set of obligations on non-genuinely critical companies.

BSA will continue to work with Congress and the Administration to narrow the criteria that have been proposed to designate critical infrastructure, and to improve the proposed designation process so that it involves industry more and provides more guarantees of due process.

c. Obligations put on critical infrastructure

We must preserve flexibility and technological innovation, which are critical to our ability to respond to cyber threats. This requires that cybersecurity obligations imposed by the government on critical infrastructure do not mandate the use of any specific technological solutions or products and, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security technologies. We will continue to work with Congress to make sure that legislation prevents the government from mandating compliance with standards that require the use by critical infrastructure companies of specific technological solutions or products.

We also must leverage recognized, internationally accepted standards developed through public and private participation, which spur the development and use of ever more secure technologies. Imposing country-specific cybersecurity standards, in particular standards developed by government agencies, would weaken cybersecurity by requiring compliance with standards that would be less flexible, less frequently updated and less adapted to each company's own cybersecurity challenges. Importantly, if the US imposes government-created, country-specific standards, we invite other countries to do the same, which would wall-off foreign markets to American companies and products. Indeed, we already face such threats in various countries.

d. Supply chain security

The development and integration of trustworthy information technology products, systems and services is one of our industry's most important responsibilities in the fight against cyber threats, and our members take it very seriously.

At this time, we do not have sufficiently detailed information to comment on the supply chain security provisions of the comprehensive bill that has been developed by the Senate. We will continue to work constructively with Congress to ensure that any legislation strengthens cybersecurity as well as our industry's global competitiveness.

e. Information sharing

Sharing information about threats and vulnerabilities and their consequences greatly contributes to more effective risk mitigation, and thus improves cybersecurity.

To date, sharing of information about threats, vulnerabilities and consequences has largely been one-way: industry shares a lot of information with the government, but relatively little of the information government gathers through its intelligence collection and investigative capabilities is shared in return.

We believe Congress should ensure that the government shares more information with the private sector. We understand that this will require overcoming persistent resistance among certain government agencies. This will not happen without engagement from government's most senior leaders, and sustained congressional oversight. The government agencies taking part in this information sharing will need appropriate direction, legal authority, and resources. Existing structures between government and industry may need to be adapted to share information in a trusted environment, but those structures provide a foundation from which to build.

Mr. GOODLATTE. Thank you, Mr. Holleyman.
Mr. Williams, welcome.

TESTIMONY OF LEIGH WILLIAMS, BITS PRESIDENT, THE FINANCIAL SERVICES ROUNDTABLE (FSR)

Mr. WILLIAMS. Thank you, Mr. Chairman, Representative Quayle, Ranking Member Watt, for the opportunity to testify on

the financial community's cybersecurity efforts, on the case for new legislation and in support of the Administration's proposal.

My name is Leigh Williams and I am President of BITS, the technology policy division of the Financial Services Roundtable. BITS addresses security, fraud, and public policy issues on behalf of 100 of the Nation's largest financial institutions, their hundreds of millions of customers, and all of the stakeholders in the financial infrastructure.

From this perspective, I can assure you that cybersecurity matters a great deal to financial institutions not because regulations require it, although they do, but because good business practices and customers require it.

At the industry level, BITS' 2011 agenda—set by chief information security officers, by CIOs and CEOs—addresses secure software, protection from malicious software, security, in social media, cloud computing, and mobile computing, secure email, and security education and awareness. While some of this work can be done within the industry, more and more requires cross-sector collaboration. For example, our sector council is working with the Treasury Department and with our financial regulators on cybersecurity exercises. We are working with law enforcement in an account takeover task force led by our Information Sharing and Analysis Center. And I thank you, Mr. Baker.

Beyond our traditional circle, with DHS, we are developing a pilot to offer expert assistance to institutions in the Cyber Operational Risk review program. Thank you, Mr. Schaffer.

And broader still, we are working with NIST to implement the National Strategy for Trusted Identities in Cyberspace. Thank you, Mr. Schwartz.

As the Committee considers legislative options, I urge Members to leverage this existing body of work and the existing controls, but also to strengthen our connections with our Federal partners and our peers in other sectors. Talking this through with my colleagues, I hear words like "integrate" and "harmonize," "align," and "reconcile." I don't hear "replace" or "substitute." And as I am sure you appreciate, I don't generally hear "add on" or "layer on."

Even given this head start and our substantial momentum, we think that cybersecurity legislation is warranted. We believe that a comprehensive bill could improve security throughout the ecosystem, including in the networks on which our institutions depend. It could strengthen the security of Federal systems and mobilize law enforcement and other Federal resources. It could spur voluntary action through safe harbors and outcome-based metrics.

Attached to my written testimony is a list of 13 policy approaches that our sector council endorsed, along with three that it found more problematic. I urge the Committee to consider these consensus recommendations of the financial community.

OMB recently transmitted to Congress the Administration's proposal to improve cybersecurity. The Financial Services Roundtable supports this legislation and we look forward to working for its passage. We support many of the provisions on their own merits, and we see the overall proposal as an important step toward building a more integrated approach.

I will structure the remainder of my testimony around the key provisions of the proposal.

We support the strengthening of criminal penalties for damage to critical computers, for committing computer fraud, and for trafficking in passwords. We also urge escalated treatment for the theft of proprietary business information.

We support the adoption of a uniform national standard for breach notification.

We strongly recommend full Federal preemption and reconciliation with the existing banking regulations.

We support exemptions, as you have heard from BSA, for data rendered unreadable and for situations in which there is no reasonable risk of harm.

We support strengthening cybersecurity authorities within DHS and codifying DHS's collaboration with the sector-specific agencies such as the Treasury Department and with sector regulators such as our banking, securities, and insurance supervisors.

We support each of the seven purposes articulated in the regulatory framework, including especially: enhancing infrastructure security, complementing currently available measures, and balancing efficiency, innovation, security, and privacy.

We think this evenhanded approach will help calibrate the effort, capitalize on existing oversight, and prevent the release of public information.

In closing, let me just underscore how much we appreciate your attention in this matter and commit that for our part we will continue to work on cybersecurity with our members and partners. We will support legislation that leverages existing protections, and we will support and help to implement the Administration's proposal.

Thank you for your time.

[The prepared statement of Mr. Williams follows:]

STATEMENT

OF

BITS PRESIDENT LEIGH WILLIAMS
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON INTELLECTUAL PROPERTY,
COMPETITION AND THE INTERNET
OF THE JUDICIARY COMMITTEE
OF THE U.S. HOUSE OF REPRESENTATIVES

OVERSIGHT HEARING ON
CYBERSECURITY: INNOVATIVE SOLUTIONS TO CHALLENGING PROBLEMS

MAY 25, 2011

TESTIMONY OF LEIGH WILLIAMS, BITS PRESIDENT

Thank you Chairman Goodlatte, Chairman Sensenbrenner, Ranking Member Watt, and Ranking Member Scott for the opportunity to testify: first, on the financial services industry's commitment to cybersecurity; second, on the need for cybersecurity legislation; and third, in support of the Administration's cybersecurity proposal.

My name is Leigh Williams and I am president of BITS. As 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.

Financial Services Commitment to Cybersecurity

Given BITS' role in the financial services community, I have a firsthand appreciation for the industry's commitment to cybersecurity. The reliability of our systems, integrity of our data, and the continued confidence of our customers are absolute requirements at the level of individual institutions and the industry as a whole. I often hear professionals at all levels - from cybersecurity professionals to chief information officers to chief executives - attest that their institutions treat cybersecurity as an internally-driven business imperative, not an externally-imposed compliance mandate. Just last week, in a small meeting of chief information security officers, one phrased it this way: "Good risk management drives good practices. Good practices then result in compliance. Not the other way around."

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 execute against our 2011 business plan, we are addressing:

- 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.

- Security training and awareness.

In several other 2011 initiatives, BITS is working closely with our private sector and public sector partners:

- 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 the Department of Homeland Security (DHS) and our Sector Specific Agency, the U.S. Department of the Treasury.
- Multiple strategies for enhancing the security of financial Internet domains - with the Internet Corporation for Assigned Names and Numbers (ICANN), the American Bankers Association (ABA) and Verisign.
- Cybersecurity exercises - with the forty-five institutions, utilities and associations of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the seventeen agencies of the Finance and Banking Information Infrastructure Committee (FBIIC).
- A comprehensive strategy for preventing, detecting and responding to account takeover - led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), and joined by a strong contingent of institutions, associations and agencies.
- 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).

In these representative initiatives from BITS' 2011 plan, and in many other efforts, the 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 Congress considers action on cybersecurity, I urge Members to be conscious of the protections 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 eco-system, 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 to my testimony is a list of thirteen policy approaches that the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) recently endorsed, along with three that it deemed problematic. For additional detail on the FSSCC's recommendations and its active role in cybersecurity, I 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. I urge the Judiciary Committee to consider the FSSCC's input, particularly in light of its 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 eco-system, with the active engagement of Sector Specific Agencies and sector regulators.

Recognizing that much of the legislative debate will begin to coalesce around the Administration's proposal, I will structure the remainder of my testimony as a brief commentary on its key provisions.

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, 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 section 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 cross-sector, uniform national standard for breach notification. Given existing state and financial services breach notification requirements, this migration will require both strong pre-emption and a reconciliation to existing regulations and definitions of covered data (please see the Federal Financial Institutions Examination Council Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice 2005-13). 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. While we recognize that additional legislative and regulatory work remains on the notification issue, we see the essential approach as highly constructive, and we look forward to heightened accountability throughout the cyber eco-system.

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 considerably more attention. 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, regardless of their geographic location or dispersion.

Conclusion

The Financial Services Roundtable and its members are fully committed to advancing cybersecurity and resiliency, and we very much appreciate your attention to this issue. To ensure ongoing progress on cybersecurity, the Roundtable will:

- Continue to facilitate collective security initiatives among its members and with its network of public and private sector partners.
- Support legislation that both improves the security of the overall cyber eco-system and leverages existing financial services protections.
- Collaborate with policymakers to refine, pass and implement the Administration's cybersecurity proposal.

Thank you for your time. I would be pleased to answer any questions you may have.

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.

Mr. GOODLATTE. Thank you, Mr. Williams.
Ms. Harris, welcome.

TESTIMONY OF LESLIE HARRIS, PRESIDENT AND CEO, CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)

Ms. HARRIS. Chairman Goodlatte, Ranking Member Watt, Members of the Subcommittee, thank you for the opportunity to testify today.

Charting a path forward on cybersecurity policy that makes meaningful improvements in security and at the same time protects privacy and innovation requires a very nuanced approach that encourages collaboration between Government and industry. One size does not fit all. Policies for Government-owned systems should be distinct from those aimed at the private sector. Government regulation needs to be limited very narrowly to critical infrastructure, and importantly particular caution has to be applied to systems like the Internet that support Americans' rights to free speech. That means as a first principle network providers—and not the Government—need to be in the business of monitoring their own networks for intrusions.

Here the Administration's bill rightly honors this principal. No Government entity needs to be involved in monitoring private communications networks as part of cybersecurity. There is no evidence that the Government can do this better and no need to move toward middle-of-the-network solutions that would put civil liberties at risk.

Second, information sharing needs to be enhanced without putting privacy at risk. There is a general agreement that more sharing is good between Government and the private sector and within industry. The White House proposal anticipates a very sweeping, albeit voluntary, information sharing regime that encourages sharing of information, including communications traffic to DHS, regardless of whether the use or disclosure of that information is otherwise restricted by law. And that means that it effectively sweeps away protections of the Wiretap Act, ECPA, FISA, FOIA—all statutes within the jurisdiction of this Committee—and many, many more. We appreciate the bill's promise of yet-to-be-articulated privacy rules, but we don't see how they can adequately police such a vast sharing regime in contrast to well understood statutory protections.

Third, the designation of critical infrastructure needs to be very narrowly tailored. Getting the government role in private cybersecurity efforts right first requires getting the designation of critical infrastructure right. Here we believe that the definition provided in the Administration's bill is overbroad and that the "debilitating impact" standard is simply too ambiguous and could sweep vast swaths of U.S. industry into the critical infrastructure fold.

Fourth, Congress should not give the President shut-off authority in cybersecurity emergencies. We certainly appreciate the White House's implicit rejection of this power in its proposal and hope that this puts this dangerous idea to rest. After the Egyptian cutoff earlier this year, it should be clear that a grant of presidential shut-down authority would set a very dangerous precedent for the world.

Fifth, the Computer Fraud and Abuse Act law needs to be tightened before we consider any new or enhanced penalties. It is a

very, very important component of our online trust framework and it has given the Federal Government authority to pursue cyber crime, hacking, and identity theft. But its vague terms have led to troubling civil and more recently criminal actions that have stretched the law far beyond what Congress intended. Indeed, some courts have interpreted unauthorized access so broadly that companies, when setting terms of service that few users will ever read, are in effect getting to determine what user conduct is criminal. So before there is any expansion of the law or increase in penalties, we need to look at those questions.

We also caution about ratcheting up penalties. The mandatory minimums in CFAA were actually repealed in the PATRIOT Act, and I think we have to know why before we put them back in. And while we have no opposition to the law being a RICO predicate, we are concerned about the consequences for civil actions where triple damages may encourage civil litigants to further pursue what we see as novel uses of this statute.

Finally, we believe the White House proposal on data breach provides a very good starting point for consideration of the Federal law. The notification trigger we think is right. The standards in the bill we think are right. But we will caution that we are talking about preempting 46 State laws, and there are some areas—for example, California has very specific protections for health information—that are not reflected. So when we are talking about the definitions in the law and when we are talking about the extent of preemption, we would urge you to be very careful.

We appreciate the opportunity to testify here today and look forward to working with this Committee on this important issue.

[The prepared statement of Ms. Harris follows:]

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

Statement of **Leslie Harris**
President and CEO
Center for Democracy & Technology

Before the House Committee on the Judiciary,
Subcommittee on Intellectual Property, Competition, and the Internet

on

Cybersecurity: Innovative Solutions to Challenging Problems

May 25, 2011

Chairmen Goodlatte and Sensenbrenner, Ranking Members Scott and Watt, and Members of the Subcommittees:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittees for examining proposals to deal with challenging cybersecurity problems. This hearing could not be more timely, coming little more than a week after the White House released its cybersecurity legislative proposal.[2] Critical parts of that legislation implicate matters that are within the jurisdiction of the Judiciary Committee.

Today, I will briefly outline existing threats to our cybersecurity and discuss how to chart a path forward that ensures protection for America's cherished rights of privacy and free expression, continues to encourage innovation, and provides for meaningful improvements in security. I will emphasize that private network operators, not the government, should monitor and secure private sector systems. I will also discuss how to enhance information sharing without eroding privacy. I will examine how the Administration's cybersecurity proposals fit this framework and note areas where they do not. And I will address the issue of

---

[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.

Presidential authority to shut down the Internet, an idea that the Administration wisely left *out* of its proposals.

CDT urges the Subcommittees 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. We urge the Subcommittees to take a careful, nuanced approach when crafting cybersecurity legislation and to avoid overbroad legislation and the attendant unintended consequences to individual rights and technological innovation.

The Cybersecurity Threat

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. In 2009, the *Wall Street Journal* reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.[3] Early last year, Google revealed that it had been the subject of a major espionage attack originating in China aimed at stealing personal information about human rights activists and Google's own proprietary information.[4] Later 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] Various criminal organizations have allegedly used malware and other invasive means to defraud U.S. financial institutions of millions of dollars.[6]

The GAO, among others, has repeatedly criticized the federal government for failing to respond adequately to this threat.[7] 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] Siobhan Gorman, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal* (April 21, 2009), http://online.wsj.com/article/SB124027491029837401.html.

[4] Ellen Nakashima, Google To Enlist NSA To Help It Ward Off Cyberattacks, *The Washington Post* (February 4, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html. Information from over 30 other technology, defense, energy, and financial firms was also compromised in related attacks.

[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?_r=1.

[6] *See, e.g.*, Federal Bureau of Investigation, New York Field Office, Press Release: Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes that Used "Zeus Trojan" and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts (September 30, 2010), http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm.

[7] *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,*

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 and those that do not must be distinguished.
- 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 designated 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 authentication of a user of an information system that controls a critical element of the electric power grid or of a user of an information system containing classified information, 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.

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.

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."[8] 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.

Network Providers – Not the Government – Should Monitor Privately Owned Networks for Intrusions

When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama said:

> *"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."*

CDT strongly agrees. No governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. Most critical infrastructure computer networks are owned and maintained by the private sector. Private system operators know their systems best and they already monitor those systems on a routine basis to detect and respond to attacks as necessary to protect their networks; it is in their business interest to continue to ramp up these defenses.

At a top line level, all of the major cybersecurity bills, including the legislation the White House has proposed, honor the Administration's pledge. But government monitoring of private-to-private communications likely will not occur through the front door. Rather, there is a possibility that government monitoring would arise 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.

Sharing Information Between the Private Sector and the Government

There is widespread agreement that the current level of cybersecurity information sharing, sharing which 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

[8] 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.

policy challenge that falls to this committee to resolve.

a. 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 and *no matter how use and disclosure of that information would otherwise be restricted by law*, so long as the entity shares it for cybersecurity purposes, makes reasonable efforts to remove irrelevant identifying information, and complies with as-yet-unwritten privacy protections.[9] 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 Foreign Intelligence Surveillance Act, the Freedom of Information Act, and the Sherman Antitrust Act – statutes within the jurisdiction of the Judiciary Committee.[10] In contrast, the leading Senate cybersecurity bill explicitly requires information sharing relating to cybersecurity incidents to adhere to the statutory schemes governing electronic surveillance.[11] Communications and other information shared with the DHS by state and local governments and by private entities would be exempt from disclosure under 5 USC 552(b)(3) and comparable state laws.

Importantly, information sharing under the Administration proposal would be voluntary, not mandatory. This is wise because giving a governmental entity mandatory authority to access private sector data that is relevant to cybersecurity[12] would create a huge loophole in electronic surveillance laws and would undermine the public-private partnership that needs to develop around cybersecurity.

In other regards, however, the White House proposal raises serious concerns. Under the White House proposal, DHS could use, retain, or further disclose the communications traffic and other information to private entities and to state and local governmental entities for cybersecurity purposes, and 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 merely 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 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 that broadly defined purpose. In addition, DHS would have substantial discretion about what to include in the privacy and civil liberties policies and procedures. Those policies and procedures would not be subject to notice and comment rulemaking under the Administrative Procedure Act. Importantly, the bill 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

[9] White House proposal, proposed Section 245 of the Homeland Security Act.

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

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

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

cybersecurity threats. However, 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")[13] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs),[14] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[15] The 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

[13] 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.

[14] 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.

[15] *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.

infrastructure and networks.[16] Industry is now represented at the NCCIC[17] 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 with industry – could ever act quickly enough 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.

Fourth, Congress must account for the significant extent to which current law gives communications service providers authority to monitor their own systems and to disclose 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.[18] This includes the authority to disclose 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[19] and customer records[20] to any governmental or private entity.[21] 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"[22] 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.[23]

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 Subcommittees 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

---

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

[17] *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.

[18] 18 U.S.C. § 2511(2)(a)(i).

[19] 18 U.S.C. § 2702(b)(3).

[20] 18 U.S.C. § 2702(c)(5).

[21] 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).

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

[23] 18 U.S.C. § 2511(2)(i).

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 need to bar the disclosure to the government of vast streams of communications data, but permit liberal disclosure of carefully defined cyberattack signatures and cyberattack attribution information. It may also need to permit disclosure of communications content that defines a method or the process of a cyberattack. 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.

Moreover, we urge the Subcommittees, before making any amendments that weaken the controls and privacy protections of the surveillance laws, to consider counterbalancing such changes with legislation to update ECPA by making its privacy protections more relevant to today's digital environment.[24] We would welcome the opportunity to work with the Subcommittees on such legislation.

The Government Should Monitor Its Own Networks for Intrusions, But Privacy Concerns Must Be Addressed

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 (DHS). Under the bill, DHS is charged broadly with engaging in cybersecurity and information infrastructure

[24] Digital Due Process, a coalition of technology companies, communications service providers, academics, think tanks, and advocacy groups spanning the political spectrum, has proposed updates to ECPA. *See* www.digitalddueprocess.org. The Center for Democracy & Technology is a leading member of DDP.

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.[25] 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 the bill does not indicate how notice would be given. 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 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 the Einstein intrusion detection and prevention system.[26] 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.

Designations of Critical Infrastructure Should be Narrowly Targeted

In terms of enhancing the security of private networks and systems, the government may assist the private sector but it should not intrude into the details of the cybersecurity planning process and it should not dictate technology standards. Private sector information technologists typically understand the operation of their own networks better than government regulators, but at the

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

[26] 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).

same time, certain agencies may have unique higher-level insights into burgeoning threats or useful defensive techniques.

First, government should concern itself only with genuinely *critical* infrastructure, and that infrastructure should be narrowly defined. A narrow definition focuses government resources where they are most needed and ensures minimal conflicts with other regulatory regimes. Such a definition also ensures that the burdens of government reporting and regulatory compliance are imposed only on private sector operators who are truly "critical" and limits impact on traditionally non-regulated entities. In this regard, the White House proposal raises very serious concerns. The proposal does little to provide specificity, defining critical infrastructure as those entities whose incapacity or disruption would cause "a debilitating impact."[27] This standard is ambiguous and could sweep vast swaths of U.S. industry into a regulatory fold.

The Senate's Cybersecurity and Internet Freedom Act of 2011 does a better job, and requires that the disruption of any critical infrastructure system 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."[28] While more precise that the definition of critical infrastructure than the White House proposal, this definition, too, would benefit from more specificity. It would be useful, for example, for the statute to define the level of economic consequences that should be considered "severe" and the duration and number of evacuations that constitute a "mass evacuation with prolonged absence." DHS has already done this in its definitions of Tier 1 and Tier 2 Critical Infrastructures and Key Resources.

Risk Management Should Target Serious Threats And Eschew Heavy-Handed Mandates

After defining which systems are critical, a risk management regime should further prioritize between levels of criticality. The White House proposal does a good job of addressing this problem by asking DHS to develop risk-based tiers and to assign entities to those tiers based on threats, vulnerabilities, and consequences of an attack.[29]

When setting a risk framework for covered critical infrastructure (recognizing that the government should be setting such frameworks, if at all, only for narrowly defined and prioritized infrastructure components), the government should strive for a consultative process rather than a command-and-control structure. The White House seems to include elements of both approaches, envisioning the government in the role of standards coordinator in consultation with the private sector and respected standards-setting bodies, but also having the power to override private sector decisions about appropriate risk frameworks.[30] DHS would ask representatives of standards-setting organizations and other entities to propose standardized frameworks for assessing risk. Importantly, "frameworks" cannot require the use of particular measures; the

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

[28] 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.

[29] White House proposal, proposed Section 3(c) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[30] *Id.* at proposed Section 4(b)(4).

decision about measures to employ is left where it belongs: with the entity to which the framework applies. After consulting with those representatives, DHS would consider whether their proposed framework reasonably assesses risks, is cost-effective, has outcome-based metrics, and will sufficiently evaluate performance. If the framework comes up short, DHS can impose its own. While this approach does require DHS consultation with the private sector, it may not give DHS sufficient incentive to consider the private sector solutions before moving on to impose its own plan.

Finally, when seeking to raise standards, the government should generally avoid mandates in favor of transparency requirements and persuasion. Mandates, through which the government directly penalizes actors who fail to meet its specifications, discourage the reporting of security incidents and put the government in the role of adversary rather than partner. Some of the Senate bills have been particularly worrisome in this regard, giving DHS open-ended regulatory powers to approve security plans and to penalize actors who fail to comply with those regulations.[31]

The White House legislative draft is an improvement over those proposals. After DHS has approved or established a risk framework, each covered entity would be required to create a plan to comply with the appropriate framework and retain an independent accredited evaluator to determine its compliance with that plan. In the event of noncompliance on the part of an entity or group of entities, DHS would have the power to demand further consultation with those entities, to issue a public statement alerting citizens to the cybersecurity deficit, or to take other unspecified action, but not to impose fines, penalties, shutdown orders, or injunctive remedies requiring particular action. The bill would also require those entities to report the results of their evaluations within their SEC filings, thus disclosing cybersecurity shortcomings to shareholders and markets. In other words, the proposal uses transparency rather than mandates as a tool to encourage compliance – an approach less likely to have some of the negative impacts on innovation that mandates have.[32]

Transparency and the Role of DOD in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency (NSA) and the newly minted Cyber Command should lead or play a central role in the government-wide cybersecurity program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government and that Cyber Command will be better resourced than DHS to do this work.

However, there is serious concern that if NSA or another DOD entity were to take the lead role in cybersecurity for civilian unclassified 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.

---

[31] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 250(c) of the Homeland Security Act (subjecting violators of Section 248 of the bill, which establishes a risk management regulatory regime, to civil penalties).

[32] The transparency called for would not tip off criminals because only high-level disclosures to the public would be made about the security plan adopted and annual performance evaluations.

Over 85% of critical infrastructure information systems are owned and operated by the private sector, which also provides much of the hardware and software on which government systems rely, including the government's classified systems. The private sector has valuable information about vulnerabilities, exploits, patches, and responses. Private sector operators may hesitate to share this information if they do not know how it will be used and whether it will be shared with competitors. Private sector cooperation with government cybersecurity effort depends on trust. A lack of transparency undermines trust and has hampered cybersecurity efforts to date.

For many reasons, openness is an essential aspect of any national cybersecurity strategy. Without transparency, there is no assurance that cybersecurity measures adequately protect privacy and civil liberties and adhere to due process and Fair Information Practice Principles. Transparency is also essential if the public is to hold the government accountable for the effectiveness of its cybersecurity measures and for any abuses that occur.

NSA and Cyber Command, for otherwise legitimate reasons, operate in a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. As a result, a DOD entity should not be given a leading role in monitoring the traffic on unclassified civilian government systems, nor in making decisions about cybersecurity as it affects such systems; its role in monitoring private sector systems should be even smaller. Instead, procedures should be developed for ensuring that whatever expertise and technology DOD has in discerning attacks is made available to a civilian agency. The September 27, 2010, Memorandum of Understanding between DHS and DOD setting forth the terms by which they would provide personnel, equipment, and facilities to increase inter-departmental collaboration and support and synchronize each other's cybersecurity operations is a good step in this direction.[33]

Presidential Authority in Cybersecurity Emergencies

There has been much discussion about whether the President or the Department of Homeland Security ought to be given 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.[34] The White House's implicit rejection of such powers in its legislative proposal should put this dangerous idea to rest.[35]

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. We know of no dispute where a critical infrastructure operator has refused to take appropriate action on its network that would justify the exercise of such a power. Operators have strong financial incentives to quarantine network elements and limit or cut off Internet traffic to particular systems when they need to do so. They know better than do government

[33] Memorandum Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity, effective September 27, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[34] The leading Senate cybersecurity bill, S. 413, 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.*

[35] Presumably, the government already has the authority to disconnect its own systems from the Internet and CDT does not challenge such authority.

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. A shut down could interfere with the flow of billions of dollars necessary for the daily functioning of the economy. It could deprive doctors of access to medical records and cripple communications among first responders in an emergency and would likely have worldwide effect because much of the world's Internet traffic flows through U.S. networks.

Even if such power over private networks were exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system.

Giving the government the power to shut down or limit Internet traffic would also create perverse incentives. Private sector operators will be reluctant to share information if they know the government could use that information 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 unfettered "shut down" authority to the President would give aid and comfort to repressive countries around the world. The government of Egypt was widely condemned when it cut off Internet services to much of its population on January 27, 2011, in order to stifle dissent. The U.S. should not now endorse such a power, even if only for cybersecurity purposes, because to do so would set a precedent other countries would cite when shutting down Internet services for other purposes.

We urge you to reject proposals to give the President or another governmental entity power to limit or shut down Internet traffic to privately held critical infrastructure systems.

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).[36] The White House seeks to further broaden the reach of the CFAA, eliminate its first-time offender provisions, make CFAA violations RICO predicates, 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 cybercrime 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

[36] 18 U.S.C. § 1030.

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,[37] the Ninth Circuit held last month 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."[38] 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 (TOS) did not allow users to create accounts under a false name. A federal judge overturned Drew's conviction under the CFAA.[39] While Drew's actions were reprehensible, they did not constitute "hacking" in any meaningful sense. Indeed, if violations of TOS 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.

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.

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

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

[38] 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.

[39] 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.

[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.

sue for triple damages for violations of that crime.[41] 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 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, clarifying the definition of "authorization" to state that only actions exceeding *code-based* authorization are sufficient to constitute a violation would improve the statute significantly.[42] 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.

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. 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.[43] The White House proposal would pre-empt those laws, which meant that it 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 offline world that incorporates the full range of Fair Information Practice Principles. The effort to

---

[41] 18 U.S.C. § 1964(c).

[42] 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.

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

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[44] – that cover health data linked to the individual's name. Further, 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, 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. 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." Some disclosures of personally identifiable information, such as health information, are harmful per se and the legislation should reflect that fact. "Harm" should be construed broadly to include reputational harm or embarrassment; with such a construction, this appears to be an effective trigger, which will avoid notification regarding truly inconsequential data breaches. Under this formulation, notice is the default and must be given *unless* there is an affirmative finding of no risk. 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.[45]

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

---

[44] 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.

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

Targeted Authentication Requirements, Rather than Broad Attribution Requirements, are the Best Way to Address Identity Issues Online

One of the most talked-about approaches to preventing and tracing cyber attacks by terrorists and others is to make it easier to identify those who access critical systems. If an attack cannot be attributed to a particular person because the person cannot be identified, it is difficult to prosecute the perpetrator or deter the attack. However, while identification will likely play a significant role in securing critical infrastructure, identity requirements should be applied judiciously to specific high-value targets and high-risk activities. Solutions that target high-risk systems and use proven authentication technologies to identify users are more likely to provide significant security benefits and less likely to produce undesirable economic and civil liberties consequences than solutions that attempt to use unproven technologies to identify and track users across the wider Internet.

Proposals to make Internet traffic broadly more attributable by changing IP address allocation standards, putting traceback mechanisms in place at routers, or even requiring the use of "Internet passports" raise serious civil liberties and economic concerns. Mandating increased attributability for routine Internet interactions could seriously compromise user privacy, chill freedom of expression online, and fundamentally limit the ways in which people use the Internet. The fact that some transactions or interactions are anonymous may *enhance* the privacy and security of those transactions. Moreover, the right to speak anonymously enjoys constitutional protection and must be preserved.[46]

On the other hand, promoting the use of better authentication technologies by the operators of specific targeted critical infrastructure systems can serve similar security requirements without economic and civil liberties harms. The use of authentication requirements should adhere to the principles of proportionality and diversity.[47] Under the proportionality principle, if a transaction has high significance and sensitivity and an authentication failure carries with it significant risk, it may be more appropriate to require authentication and the collection of more sensitive information to authenticate. Conversely, certain transactions do not need high degrees of authentication, or any at all. This principle applies in both the private and public sectors, but private sector operators – who know their systems best – are in the best position to decide what level of identity and authentication should be required for their own systems and transactions, depending on the degree of risk posed and the degree of trust that is called for. Narrowly targeting authentication requirements only to the most critical systems helps ensure that the economic burden of compliance is minimized and that privacy and free speech are protected.

---

[46] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

[47] CDT has outlined these and other Privacy Principles for Identity in the Digital Age. Version 1.4 of the principles, released in December 2007, can be found here: http://www.cdt.org/security/identity/20080108idprinciples.pdf. The privacy principles for identity that extend beyond proportionality and diversity are based on Fair Information Practice Principles, and include specifying the purpose for the system being used, limiting the use and the retention period of personal information collected, giving individuals control over and choice about identifiers needed to enroll in a system (to the extent possible), providing notice about the collection and use of personally identifiable information, securing against misuse of the information provided, requiring accountability for data processors, providing users access to their own data, and ensuring data quality.

Under the diversity principle, users should have identification and enrollment options that function like keys on a key ring, with different identities for different purposes.[48] One model that holds great promise is the "user-centric" federated identity model, in which the user logs into a Web site through a third party identity provider, who passes on information at the user's request to the Web site in order to authenticate the user. The recently released National Strategy for Trusted Identities in Cyberspace (NSTIC) does an excellent job of advancing this model.[49] It envisions an identity eco-system led by various private sector identity providers rather than a "government ID for the Internet." It also accounts for the need to have a range of levels of assurance for interaction on the Internet, ranging from completely anonymous to highly assured.

Conclusion

We appreciate the opportunity to testify about innovative solutions to cybersecurity challenges. The White House proposal raises critical issues that fall squarely within the Judiciary Committee's jurisdiction and within the jurisdiction of the Subcommittees. 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.

[48] *See* Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age* (December 2007), http://www.cdt.org/security/identity/20080108idprinciples.pdf.

[49] White House, National Strategy for Trusted Identities in Cyberspace (April 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Mr. GOODLATTE. Thank you, Ms. Harris.

I will begin the questioning, and my first question is directed to you, Mr. Holleyman.

To what extent has the Administration worked with the technology sector and incorporated their best practices into the cybersecurity legislative proposal?

Mr. HOLLEYMAN. We have worked closely with the Administration throughout this process, have particularly worked closely with NIST over a period of time. I think, in large part, the Administration's proposals reflect ones that we would endorse. There are other issues where we have proposed recommended changes, as we sub-

mitted in our testimony and a few issues that have not been resolved. So I think that the inclusion of this effort from the Administration has been helpful and it is good to see them come forward with a concrete proposal.

Mr. GOODLATTE. How can Congress encourage innovative solutions to combat this dynamic problem and avoid the one-size-fits-all regulation that Ms. Harris and others have expressed concern about?

Mr. HOLLEYMAN. By making sure that there are technology neutrality provisions that are always taken into place. There is no one-size-fits-all technology that will work for every solution, every customer, every government. We need to have the flexibility to adapt and use new technologies as the nature of the crimes adapt. So maintaining that principle is important.

And I think, secondly, by ensuring that the level of Federal resources against cyber crime can be escalated in a way that there is a greater deterrent, because we are all at risk, and the Federal Government has a unique role in fighting cyber crime.

Mr. GOODLATTE. Mr. Williams, what are banks proactively doing to ensure that critical data is protected from hackers and economic espionage by foreign competitors?

Mr. WILLIAMS. Individual institutions are doing a great deal. They each have programs that are embedded within their operational risk and their general risk management programs, some of which are subject to review by regulators of the banking securities or the insurance industries, others of which exist solely on the basis of it being good practice. They also conduct, through BITS and many other coalitions, a great deal of industry-level work to ensure some consistency throughout the industry and to help connect the industry—the sector with other sectors.

Mr. GOODLATTE. When there are data breaches, how are they generally handled? Is it standard practice to provide public notification or inform Federal authorities or both?

Mr. WILLIAMS. There are actually already, within the banking subsector of financial services, uniform national standards for preparing for, responding to, and notifying of breaches, and over the last several years, as the industry has gravitated toward that uniform approach, we have found it to be very effective.

Mr. GOODLATTE. Ms. Harris, do you think it should be Government or the private sector to take the lead in determining best practices for cybersecurity?

Ms. HARRIS. I think it should be the private sector, and I think in this regard, the Administration's bill does a very good job of putting the private sector in the lead for developing these sectoral risk plans and then allowing the companies to develop their own individual plans. Our only concern is making sure that the definitions in this bill are sufficiently precise so that as we go down the road to deciding which sectors are cybersecurity infrastructure, critical infrastructure, we don't come up with a definition that is overbroad.

I think on the second part, whether they have gotten a good balance between public and private, I think they have done a pretty good job, but that is once you have been designated "critical infra-

structure." Our concern is not to have too many industries swept into that basket.

Mr. GOODLATTE. You are all saying that there is a good deal of collaboration in writing this legislation, and that is good to hear.

What can the Congress do to strengthen the ongoing cooperation between private enterprise and the Federal Government on cybersecurity? Does anybody want to tackle that first? Mr. Holleyman?

Mr. HOLLEYMAN. Two things. One is to enable the private sector to share more information about the specific nature of threats, but we also very much feel that there needs to be mechanisms by which the Federal Government shares information with companies, particularly in the security space, about the nature of the threats so that we can work in closer partnership. Generally our companies do share a lot of information. We think this proposed legislation would help foster a better climate for more, but we would like to see more from the Federal Government in appropriate circumstances that could be shared with industry.

Mr. GOODLATTE. Thank you.

Mr. Williams?

Mr. WILLIAMS. Mr. Chairman, I would offer two responses.

First, I was very encouraged in the first panel to hear the phrase "providing opportunities for voluntary information sharing." We think that they should be voluntary but enabling those opportunities we think is very important.

The second thing I might say is that we already have very strong information sharing within the financial services sphere. Part of the reason, a great deal of the motivation, for our supporting this comprehensive legislation is to extend beyond our sphere, to extend to our service providers, to our customers, to agencies other than our banking regulators to ensure that the overall ecosystem is protected.

Mr. GOODLATTE. Thank you.

Ms. Harris?

Ms. HARRIS. So I agree that data sharing is important. We have some very specific concerns, and those concerns are in the way this law is constructed. Rather than trying to figure out what aspects of the law, particularly ECPA, may not be adequate to allow more sharing to occur, it simply sweeps away all of these laws in favor of this broad voluntary mechanism.

So I think that this Committee is the right Committee to try to figure out whether we can pinpoint in a serious way what is the legal barrier that exists right now in our Government information sharing laws and how do we narrowly fix that without basically throwing out all those laws and other Federal and State laws that touch on privacy. I just think this is the right Committee to do that and that this is a big challenge. It is, I think, not the right approach to simply say, "notwithstanding any other provision," and sweep everything away. It is this Committee's laws. It is health laws. It is Gramm-Leach-Bliley. It goes on and on, and I don't think anybody can tell us what the implications of that might be.

And second, this is a law enforcement Committee. I guess, no, it is not because we switched Committees here. And getting a law enforcement piece right is important. And I think I have mentioned

some of the changes that I think are necessary in the CFAA before we start to take a look at penalties and other changes.

Mr. GOODLATTE. Thank you.

The gentleman from North Carolina, Mr. Watt, is recognized.

Mr. WATT. Thank you, Mr. Chairman.

I am trying to get to this question that Ms. Harris has touched upon here, the definition. And I think that is what is troubling me here and probably what is troubling the Chairman is where the divide is between what the Government should be doing and taking control of and what is outside what the Government should be doing.

So I am looking here closely at the legislation, and there is section 242 which defines "critical infrastructure" that refers us back to the emergency preparedness statute which defines the word "critical infrastructure." And then there is a separate section which defines something new, I take it, which is called "critical information infrastructure," which goes beyond the emergency preparedness thing.

I think we have probably all gotten comfortable with the emergency preparedness part of this. That is the Government's role clearly. I am not even second-guessing that. That has been in the statute.

But this definition of "critical information infrastructure," a new term in this statute, seems to be very, very broad. And I think we have got probably some very serious work to do.

Can you help me, Mr. Holleyman, kind of understand what you perceive to be critical information infrastructure? I mean, you are familiar with these two things that I just talked about. Right? Have you looked at the statute?

Mr. HOLLEYMAN. I am familiar with what you are talking about, but I can't offer today a recommendation. I would like to get back to you with some thoughts.

Mr. WATT. And I am going to tell you the one thing that is troubling here—and I raised it with the first panel because once you start defining "critical information infrastructure," if it is defined too broadly, it has a lot of implications. And then you start talking about preempting State laws with respect to any critical information infrastructure, then you get into a whole other segment of things. Then when you start saying the Government can demand or request certain information and provide legal immunity for providing that information, you get into a whole different set. And that is very delicate territory.

Is my personal information, if it is breached in a corporate computer—is that critical information infrastructure or is it outside? Mr. Williams? Let's put it in the financial services context. I serve on the Financial Services Committee too. So I am very familiar with this. We have debating this for a long time. Is a breach of my personal information by—somebody craps into Bank of America or Mechanics and Farmers Bank, which is where I bank, and breaches their—and they get my personal—does that make that critical information infrastructure?

Mr. WILLIAMS. If I might answer your direct question and maybe extend it a little bit. I think the direct answer is yes. If your personal information—collected, aggregated with the personal infor-

mation of a lot of the other customers of a particular bank—is breached, it absolutely constitutes what I think the legislation calls a risk to critical economic security of the United States. If it is any one person, perhaps not, but in the aggregate absolutely.

In extension, I would say that within financial services, we have begun to think about what is and is not critical. As you know, institutions now are subject to a designation by the Treasury and the Financial Services Oversight Council of being systemically important which we could think of as financially systemically important or operationally systemically important.

We also, outside of our industry, have begun——

Mr. WATT. Okay. Well, let me just take this one step further. My personal information, aggregated with other people's personal information, can bring down the whole system. I acknowledge that. But does that give the Federal Government the right to preempt a State law that says it will protect my personal information? Where does that fall?

Mr. WILLIAMS. I think in the narrowest sense, our banking regulators have already said that we need to have notification requirements and security requirements that protect single individuals' information at the Federal level.

Mr. WATT. Yes. We are fighting that battle. I was involved in drawing the preemption language in Dodd-Frank. It was an absolute nightmare. I had consumer groups in the room. I had bankers in the room. The Senate took it and referred it to some case law, some case that had been decided by the Supreme Court, and they are still fighting about what is preempted and what is not preempted.

This is much, much, much broader than that, and we couldn't even agree on what the Federal preemption standards should be for the financial services bill. This is so much broader than what we were talking about in the financial services bill. I mean, something that is so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, that is fine.

But when you talk about national economic security or national public health or safety, this is a very, very broad definition of how you are defining that. And I think it is that discomfort with the Federal Government being too much in that space that people start to say are we setting up a Big Brother system here where the tail is wagging the dog basically.

I am sure people have been working on this, but we have got a lot of work to do, I think, on this definition before we can get the public comfortable with having Homeland Security call up a company and demand that it give—well, they say they are not demanding. They are just requesting it. But you heard Mr. Baker say when the Government requests and you couple that with giving immunity to the companies for providing the information to the Government, then you are right back to where we were under the PATRIOT Act. And people get very uncomfortable with the Government being so powerful that it can then call up and demand certain information and then provide immunity for somebody when they provide that information because they don't necessarily even want

the Government to have immunity in that case if they violate the standard that is applicable.

It is a very difficult line that we are walking here. We can't define it today. I am way over my time, but I think that is the most troubling aspect of what we have got to deal with here, and it is providing discomfort on the left and it will provide discomfort on the far right. That is when I used to jokingly say I would quite often back around the circle into Jesse Helms. I would be backing from the left and he would be backing from the right, and all of a sudden, we would be standing in the same place because both of us were suspicious of too powerful a Government. And that is where we could get if we are not careful.

Mr. Chairman, I am on a soapbox, so I am going to yield back.

Mr. GOODLATTE. Well, I have enjoyed standing here listening to you.

The gentleman from Arizona, Mr. Quayle, is recognized for 5 minutes.

Mr. QUAYLE. Thank you, Mr. Chairman.

Mr. Williams and Mr. Holleyman, I am kind of going along the same lines. My concern is that with the broad definition for the covered critical infrastructure and how it is going to apply to various small business, medium-sized businesses that are starting to grow and then their inability to be able to cover those expenses or at least they might be eating into their margins because they don't have the ability like some of the other large financial institutions that have the capital to be able to comply with these various regulations.

How will this, because it is so broad—and I know that we are talking about having to tighten up the language and all, but my concern is how are we going to be able to make it so that we are not going to be inhibiting growth in the private sector. Because if the regulations are overly burdensome, we are going to have a situation where companies are going to look to see their cost-benefit analysis of whether they are going to grow and then fall under that critical infrastructure or stay the same size and not have to comply. That is one of my biggest concerns, because this is overbroad and how that is going to affect growth in the private sector.

Mr. WILLIAMS. I absolutely share your interest in setting those criteria. I will leave it to the judgment of the Congress how much of the specificity belongs in the legislation, in regulation, or in judicial reviews as we heard earlier on this point and on several other points.

What I will say is at least in financial services, we have begun to set a fairly high threshold. So the systemically important financial institutions are really the largest and the most interconnected. The operationally significant financial utilities are a small number of highly connected organizations that I don't think would qualify in the small business category that you——

Mr. QUAYLE. Kind of running on the same lines, if the private sector is already addressing the situation, if like you were saying, large financial institutions—you know, a lot of their business is made at lightning speed transactions and they make or don't make money based on that. And so having that cybersecurity infrastruc-

ture within that framework is important to them, but they are doing it on their own initiative.

So if you are saying that you are already having a lot of these critical pieces of infrastructure doing it without the regulatory framework in place, why don't we just leave it to the people to do best practices and then be able to make their own determination on what level? Because quite frankly, I think that somebody who is banking with a Bank of America or a Chase or whatever—they will be looking to those that have the cybersecurity framework in place as a way to make a decision in the private sector and let the market kind of take that approach.

Mr. WILLIAMS. It does happen, we think, with a lot of companies in a lot of sectors, many of whom are business partners to financial providers, but we think it happens unevenly. So we depend on electric utilities. We depend on the telecom networks. We depend on software providers, many of whom are strong and responsible but not all of whom operate with the same level of resilience. We think raising that general bar makes a lot of sense.

Mr. QUAYLE. Okay.

And Mr. Holleyman, you were mentioning a lot of the trademark infringement that happens in the Internet and elsewhere. That is rampant. Anytime you do a search, you can find copyright infringed products out there.

But is this the right piece of legislation to be going for that? Wouldn't it be a lot more effective to have independent legislation that is outside of this larger regulatory framework to address that situation? Because it doesn't seem like it goes really hand in hand.

Mr. HOLLEYMAN. Well, I think that is a great question. We do think that this is a piece of legislation that should address the cyber framework. I was drawing into that, however, one other area that this Committee has responsibility for which is the area around intellectual property protection but specifically the nature of software because fully a third of the software that is used illegally and downloaded off the Internet contains malware. And malware is providing a penetration in the systems that has a pervasive impact well beyond the intellectual property or the software industry.

And I was encouraging this Committee to encourage the Administration to issue the executive order that requires Federal contractors to use only legal software in the same way that is required of Federal agencies, not only because it is important for intellectual property protection, but because the same type of vulnerabilities are being introduced into the Federal network when Federal contractors are using illegal software which oftentimes contains the type of malware that poses a cybersecurity risk. So I am linking the two issues.

Mr. QUAYLE. Thank you very much.

I yield back.

Mr. GOODLATTE. I thank the gentleman.

The Chair recognizes the gentlewoman from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

First, my apologies for not being here for this whole hearing. We had a markup in the House Administration Committee that I had

to go to, but I have read all the testimony and it is very, very helpful.

Ms. Harris, your testimony relative to the standards is very, very useful.

And Bob—I mean, Mr. Holleyman—your preemption issue is an important one. It is difficult, as the Ranking Member has discussed, but I think we are going to have to address it in terms of data breaches because the current situation is chaotic. And that is going to be hard to do since all of us—States have been aggressive about privacy. We are not going to be able to go home if we don't maintain some similar types of standards.

I credit the Administration for working with the technology sector, but we are a long ways from where we are going to need to be on this. The idea that we would waive all other law, provide immunity. I mean, when the Government goes to the private sector and asks for something, it is more than just asking. I mean, there is an obligation. We have seen that in many other contexts. There is no liability. Even with liability, companies respond. If there is no liability and the standards are as vague as this, we have created a big Government nightmare, and we just can't go there.

On the other hand, cybersecurity and the threat to our cyber infrastructure is very real. And I am wondering, as we move forward, if we can make some distinctions not just on the nature of the activity but the origin of the threats because there are different levels based on where the threat is coming from.

I am not an anti-government person, but I am mindful that the Department of Homeland Security for over a year and a half maintained a miniature golf site on its list of critical infrastructure and wouldn't take it off. So let's not be believing that the Department knows everything there is to know about the critical infrastructure threat that we face. We tend to over-categorize things in Government, and if we do that in this case, we will see Government encroaching on really what should be the private sector's primary responsibility and certainly that of free Americans to be able to communicate without fear of intrusion or monitoring by their own Government.

So those are big-deal defects in what has been presented so far, and I am hearing some bipartisan concern along those lines. And I am confident that the Administration will want to work with us to fix those items.

I am just wondering. Maybe all of you can comment on this. To some extent, the Administration's proposal seems to put the Government at sort of the center of the cybersecurity information sharing. And I think it is true that the private sector has given up more than they have gotten back, and that has to change. But I am wondering whether that is really optimal, whether we want the Federal Government to have that man-in-the-middle centrality role or whether there is some other way to structure it that might be more nimble.

Do you have any comment on that, the three of you?

Ms. HARRIS. So that is a question that we have been asking as well, as to whether or not all information in and all information out, which has been the model, really is the most nimble way to share information and there are a variety of private sector sharing

groups going on. But I think it is worth exploring whether or not that is—I mean, we have information sharing already set up in the Federal Government, and in fact, in the last couple of years, that has improved, I think, quite a bit.

But, obviously, the civil liberties issues are ratcheted up when all sharing has to go through the Government or is encouraged to go through the Government. I need a better understanding of sort of the value added. Obviously, the Government needs that information for its own purposes, but the question is whether or not everybody has to go to "go" first before they deal with each other.

I know there is sectoral sharing. I find this very difficult.

Ms. LOFGREN. If I can just add in one other element, which is some sectors that are, in fact, critical that an attack would deal with systems and create cascading failures have taken significant steps to protect themselves, the financial sector among them. Other sectors, not so much. The ISACs—you know, some have worked well, some not so well.

And so maybe one thing that we could do—I don't really see a robust section here—is really even the assessment of—you know, maybe it is the liability that ought to be imposed on certain sectors—and they tend not to be the technology sector—where they have not taken the minimal steps necessary to protect themselves, and their lack of doing so puts the Nation at risk. Maybe we ought to be doing some incentives in the negative way for some of those sectors where the catastrophe awaits us.

Mr. WILLIAMS. I certainly agree, ma'am, that the private sector should be the primary locus of all of this work. We within financial services, and I suspect in many other sectors, have utilities that are entirely private and we have the ISACs that are semi-private. And a great deal of the work occurs in all of those places. There should be incentives and disincentives that strengthen all of that private sector work.

I suspect that if we create more resources on the Federal side and strengthen a hub of information sharing on the Federal side, it will still allow for that rich private work to take place. I would never support substituting all of the dispersed private effort for a centralized Government effort, but I suspect that there is room for both.

Mr. HOLLEYMAN. Ms. Lofgren, if I can mention two ideas.

One is we think that the most important role for the Federal Government is to serve as a convener by bringing in the interested parties together. We think in particular NIST and others have done a great job in taking on that role.

Secondly, where critical infrastructure may ultimately be defined, we think there are two hallmarks to it. One, it needs to be a narrow definition, and second, there needs to be flexibility around how entities in critical infrastructure use security products to create the kind of security and deal with the evolving nature of the threats.

Ms. LOFGREN. I know my time is up, but in some cases that includes—our own Government has failed to do even the minimal thing. I remember a hearing on US-VISIT in the Homeland Security Committee where we learned for the first time that they hadn't

even deployed intrusion detection software. I mean, it was stunning.

So we have a long way to go, but this bill also has a long way to go.

And I thank the Chairman for indulging me over my 5 minutes and yield back.

Mr. GOODLATTE. I thank the gentlewoman.

And I am pleased to recognize the gentlewoman from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, thank you very much.

To the witnesses, I was detained. We held, Mr. Chairman, a hearing in Homeland Security that actually overlapped some of the very questions that are being raised here from a different perspective, and that is the in-depth use of cyber sites by individuals intending to do us harm. So I think it is a two-edged sword or focus in terms of the protection of data, but as well as protection of the American homeland. And I raise my questions accordingly.

And I would just like to put the President's remarks in the record by reading them in part. His statement was: "We count on computer networks to deliver our oil and gas, our power, and our water, rely on them for public transportation, air traffic control. But just as we failed in the past to invest in our physical infrastructure, our roads, our bridges, and rails, we have failed to invest in the security of our digital infrastructure and the status quo is not acceptable." And I join him in that, which is I guess the basis of his plan and initiative.

I want to start with Mr. Williams because I might not have heard you correctly when you seemed to have been arguing against a central Government plan which I took to be focused on how to structure our security and data protection versus the private sector involvement. Can you just expand on what you were saying there, please?

Mr. WILLIAMS. Yes, ma'am. We certainly believe that expanded authorities in the Department of Homeland Security and an expanded role of the Government are appropriate. We think that this is important, as we go through this arc that Mr. Holleyman described where we have gone from very simple, unsophisticated hackers to much more sophisticated attacks. This warrants a more collective approach to protecting the overall ecosystem.

What I would say—and maybe this is where that has softened a bit—is that even if we build up that center, even if we build those resources and improve our ability to take advantage of that hub and that convening authority, we will still very much have a widely dispersed expertise and set of resources that are at the disposal of companies. Individual companies, their utilities, their service providers, their nonprofits, their coalitions I think probably will still be the primary gravitational center of the work.

Ms. JACKSON LEE. So it is important for the private sector to develop cutting edge technology simply to provide protection. Is that what you are saying? You should continue to do research and develop that next level of software that provides that protection.

Mr. WILLIAMS. Absolutely, absolutely.

Ms. JACKSON LEE. Let me follow up on some of the materials that we received in the previous hearing that spoke about some of

the either unknown or unattended to sites where the Taliban in Afghanistan can, without hindrance, have friendly conversations that may even intrude into the United States.

Let me ask all of you. Do you have an intensity with your particular companies, those you represent where you are aware of that usage of sites seemingly unimpeded? Do you cooperate with, for example, the FBI? Do you believe the FBI has sufficient tools on this? And I am saying this in the backdrop of a very sensitive concern about civil liberties and civil rights. So I am particularly concerned about sites that are international that are able to pierce the cyberspace that we have. Do you want to start, Mr. Holleyman?

Mr. HOLLEYMAN. Ms. Jackson Lee, I don't have any information about the specific narrow question you posed. Certainly in a variety of cyber crime activities, companies in the software industry do cooperate with law enforcement, but I can't comment on your specific question.

Ms. JACKSON LEE. So you are not aware——

Mr. HOLLEYMAN. I am personally not in my role as the president of our association.

Ms. JACKSON LEE. Mr. Williams?

Mr. WILLIAMS. We do work very actively with law enforcement at every level with both the U.S. authorities and with non-U.S. authorities to ensure that our systems—financial services systems—are not used for malicious purposes, to protect the intellectual property that lives in those systems, to protect the personally sensitive information that is in those systems. We have a lot of good motivations for working actively with people in the private sector and the public sector to protect the financial infrastructure.

Ms. JACKSON LEE. Do you have any comment, Ms. Harris?

Ms. HARRIS. Well, I represent a civil liberties organization.

Ms. JACKSON LEE. Right. That is why I asked if you had a comment.

Ms. HARRIS. Beyond that——

Ms. JACKSON LEE. I will move to my next question. Thank you.

Ms. HARRIS. Okay.

Ms. JACKSON LEE. The next question is the current trend of technology is to place information onto the cloud of third party operating systems and allows phones and computers to access this information. How does this rapidly growing dependence on storing information remotely in the cloud impact the steps individuals, businesses, and the Government should take to enhance cybersecurity? And how will the Government address jurisdictional issues? I don't want to ask about the Government, but what are you all doing with respect to that concept?

Mr. HOLLEYMAN. Well, from a software industry perspective, there are several things we are doing. One is companies that are providing cloud services or hosting very much realize that the security associated with their cloud offerings is going to be critical not only to comply with a variety of laws, but also to gain customer confidence. It is probably one of the most important things that you can do, and they are very active at the top of the list.

Second is that we are building awareness of the fact that customers should be asking questions about where their data is hosted and the level of security that that cloud service provides.

And finally, if a cloud offering is, in fact, secure, we believe it could provide a higher level of security than the very dispersed nature of servers and networks that exist today. So we are trying to make it clear that there is nothing inherently problematic about storing information in the cloud. In fact, it could be better in many circumstances, but you have to ask the questions about how providers are securing information and what steps are they taking.

Mr. WILLIAMS. We have specialists in a lot of different disciplines active in our program, and people from every one of those disciplines have asked about and worked on cloud. So we have security specialists thinking about what the marginal security requirements would be and what the security improvements might be coming from a cloud-based infrastructure.

We have people who work with service providers who are asking what contractual provisions can help protect information and systems in the cloud in a way that might not have been contemplated when servers were all in one location.

And we have people who work on public policy thinking about what the right regulatory framework would be for looking at cloud where geological boundaries make a little bit less sense.

Everyone has an interest in it and many of those interests, we hope, will lead to cloud being not something that would ever degrade security or degrade resiliency but would improve it.

Ms. JACKSON LEE. So you are not running away from that. The business community is actively engaged.

Mr. WILLIAMS. We are absolutely engaged. I can tell you that within financial services, firms are very reluctant to move their information to a public cloud where the resiliency standards are set on the basis of what is publicly appropriate for relatively nonsensitive information. They are much more likely to use proprietary clouds or industry-specific or regional clouds where they can have elevated controls in place.

Mr. GOODLATTE. The time of the gentlewoman has expired.

Ms. JACKSON LEE. Ms. Harris, was trying to answer. Could she——

Mr. GOODLATTE. Without objection, the gentlewoman will be granted an additional minute.

Ms. JACKSON LEE. I thank the gentleman.

Ms. HARRIS. I think that security in the cloud certainly with companies that are providing applications and storage and other services, cloud services, to business, security is good and getting better.

I think that the unanswered question here is security and privacy and other rights for consumers in the cloud, and that is certainly beyond the scope of this hearing. But it is far less clear to me that as consumers are encouraged to move their information to the cloud, that they can be guaranteed the same level of security protections, nor can they be guaranteed the same level of privacy protections. Our constitutional protections, our Fourth Amendment protections, our ECPA protections have been outstripped by technology. We don't have consumer privacy laws in this country that broadly apply to data. So there are a lot of issues for consumers in the cloud that go sort of beyond what business has to face.

Ms. JACKSON LEE. I thank the Chairman very much. Mr. Chairman, I just want to make this one comment, and I know that we

are speaking of software, but I really appreciate this hearing. I am sorry I was not here for its entirety. But there really is—besides the constitutional issues—Ms. Harris, I am not ignoring that and the civil liberties. There really are real challenges for cybersecurity and particularly unhosted sites, and I would imagine that there would be overlap between Judiciary and Homeland Security on these issues that have to do with terrorism.

Mr. GOODLATTE. Undoubtedly there is.

Ms. JACKSON LEE. I yield back.

Mr. GOODLATTE. I have one additional question. I direct it to Mr. Holleyman an Mr. Williams.

How worried is the tech industry about state-sponsored hacking and theft?

Mr. HOLLEYMAN. The tech industry is certainly very worried. It is probably one of the fastest growing forms of risk. I can't quantify the extent today, but it is certainly something that we work closely with Government in trying to identify where those risks may be occurring.

Mr. GOODLATTE. Mr. Williams?

Mr. WILLIAMS. The financial services industry is very focused on the most sophisticated threats with or without attribution, whether they happen to be state-sponsored or sponsored by some other malicious actor. We are very focused on ensuring that the simplest, most unsophisticated threats are absolutely taken care of, but we are more and more focused on this more sophisticated tier.

Mr. GOODLATTE. Thank you.

Mr. Watt?

Mr. WATT. I think I might pass except to observe that having dealt with the systemic risk issue, it seems to me that that is in the financial services sector. This bill seems to me to be putting Homeland Security in a much, much, much more powerful position on a much, much broader range of issues than we dealt with with just financial services' systemic risk.

And one might wonder at some point whether the director of Homeland Security is a lot more powerful than the chairman of the Federal Reserve. I don't ask that. I was just wondering aloud. Just wondering aloud. We will talk off the record.

Thank you, Mr. Chairman.

Mr. GOODLATTE. I thank the gentleman.

And I want to thank all of our witnesses. It has been a very helpful contribution to this hearing. In fact, the entire hearing has been very useful. It is very clear that this is a wide-ranging subject that, in terms of the Congress tackling it, is going to involve a lot of input from a lot of Committees. But I think this Committee has a critical role to play both the Intellectual Property, Competition and the Internet Subcommittee, as well as the Crime Subcommittee, and we look forward to working together to accomplish some good legislation that would buttress the work of the Administration and certainly give guidance to the private sector.

So without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond to as promptly as they can so that their answers may be made a part of the record.

Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

With that, I would again like to thank our witnesses and declare the hearing adjourned.

[Whereupon, at 12:27 p.m., the Subcommittee was adjourned.]

○