CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND PUBLIC-SECTOR RESPONSES

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 28, 2012

Serial No. 112–134

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
78–432 PDF WASHINGTON : 2013

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 ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon
Chairman

LEE TERRY, Nebraska
Vice Chairman
CLIFF STEARNS, Florida
JOHN SHIMKUS, Illinois
MARY BONO MACK, California
MIKE ROGERS, Michigan
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

ANNA G. ESHOO, California
Ranking Member
EDWARD J. MARKEY, Massachusetts
MICHAEL F. DOYLE, Pennsylvania
DORIS O. MATSUI, California
JOHN BARROW, Georgia
DONNA M. CHRISTENSEN, Virgin Islands
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
DIANA DeGETTE, Colorado
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

CONTENTS

Witnesses

Submitted Material

CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND PUBLIC–SECTOR RESPONSES

WEDNESDAY, MARCH 28, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in room 2322 of the Rayburn House Office Building, Hon. Greg Walden (chairman of the subcommittee) presiding.

Members present: Representatives Walden, Terry, Stearns, Shimkus, Bono Mack, Blackburn, Bass, Latta, Guthrie, Kinzinger, Eshoo, Matsui, Barrow, Dingell, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight; Ray Baum, Senior Policy Advisor/Director of Coalitions; Nicholas Degani, FCC Detailee; Andy Duberstein, Deputy Press Secretary; Neil Fried, Chief Counsel, Communications and Technology; Debbee Keller, Press Secretary; Katie Novaria, Legislative Clerk; and David Redl, Counsel, Communications and Technology; Shawn Chang, Democratic Senior Counsel; Jeff Cohen, FCC Detailee; Roger Sherman, Democratic Chief Counsel; and Kara van Stralen, Democratic Special Assistant.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Good morning. The Subcommittee on Communications and the Internet will come to order. The title of today's hearing is "Cybersecurity: Threats to Communications Networks and Public-Sector Responses."

Heeding the call of the House Republican Cybersecurity Task Force appointed by the Speaker, this subcommittee has embarked on a series of hearings, as most of you are aware, to get a complete picture of the cybersecurity challenges that face our Nation. Today is the third of our hearings on this topic, having already heard from witnesses in our previous hearings on the concerns of the private-sector security firms helping to secure communications networks from cyber threats as well as the network operators that must protect their networks while providing the broadband services that have become the fuel of our economy. Those hearings provided us with a lot of very, very valuable information. We appreciate the witnesses who testified. This hearing continues our subcommittee's review of cybersecurity issues with a focus on the public sector.

In order to further investigate the complex issues that surround any discussion of cybersecurity, I recently asked a number of my subcommittee colleagues to serve on a bipartisan working group tasked with gathering additional information. My vice chairman, Mr. Terry, and Ranking Member Eshoo have graciously served as co-chairs of the working group for the last few weeks, and I am very appreciative of their work. The group also included Representatives Doyle, Matsui, Kinzinger, and Latta. The members of the working group and their staffs have met with a number of industry stakeholders, and throughout their discussions a consistent theme has emerged: the need for the government and the private sector to work together to address cybersecurity. The findings of the working group are consistent with the message we have heard in our hearings on this matter from the private=sector perspective.

Today, we hear from some of the agencies within our government that are working to meet these threats, both in terms of what is being done to promote cybersecurity as well as how we can better secure our Nation's communications networks. In this hearing, we are privileged to have five witnesses that represent parts of the government that work to address the complex cybersecurity issues our country faces every day. The work being done by these government agencies to help address cybersecurity is just the tip of the iceberg of what we can achieve when our private-sector innovation and public-sector resources are put to a common task. That is why I am a co-sponsor of H.R. 3523, which is the Cyber Intelligence Sharing and Protection Act. This bipartisan bill introduced by my Communications and Technology colleague and chairman of the House Permanent Select Committee on Intelligence, Mike Rogers. H.R. 3523 makes commonsense changes to the way our government and the private sector share cyber intelligence without compromising either the commercial broadband providers or the integrity of the intelligence community.

Similarly, the good work being done by industry stakeholders at the FCC on the Communications Security, Reliability and Interoperability Council, or CSRIC, to bring voluntary best practices to bear on the security of commercial networks is another example of the type of public-private cooperation that I think will achieve results without mandates. It looks very similar to the Australian model that received favorable reviews at one of our previous hearings. To remain nimble and effective, codes of conduct like these should remain voluntary and should involve all stakeholders in the Internet ecosystem, not just the ISPs.

In addition to hearing from these agencies on the good work that they are doing, I also expect to hear how you think we can improve the cooperation between the Federal Government and private industry as they work to combat cyber threats. Having heard from the private sector, today's public-sector perspective will give the members of the subcommittee a more complete picture of the cybersecurity landscape.

I thank the panelists for your testimony today. I look forward to a lively discussion of these issues.

[The prepared statement of Mr. Walden follows:]

Statement of the Honorable Greg Walden
Subcommittee on Communications and Technology
Hearing on "Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
March 28, 2012

(As Prepared for Delivery)

Heeding the call of the House Republican Cybersecurity Task Force that recommended the review of cybersecurity issues within our jurisdiction, this subcommittee has embarked on a series of hearings to get a complete picture of the cybersecurity challenges our nation faces. Today is the third of our hearings on this topic, having already heard from witnesses in our previous hearings on the concerns of the private sector security firms helping to secure communications networks from cyberthreats as well as the network operators that must protect their networks while providing the broadband services that have become the fuel of our economy. Those hearings provided us with valuable information and even some potential solutions. This hearing continues our subcommittee's review of cybersecurity issues with a focus on the public sector.

In order to further investigate the complex issues that surround any discussion of cybersecurity outside of a hearing context, I recently asked a number of my subcommittee colleagues to serve on a bi-partisan working group tasked with gathering additional information. My vice-chairman, Mr. Terry, and the ranking member have graciously served as co-chairs of the working group for the last few weeks. The members of the working group and their staffs have met with a number of industry stakeholders and throughout their discussions a consistent theme has emerged: the need for the government and the private sector to work together to address cybersecurity. The findings of the working group are consistent with the message we have heard in our hearings on this matter from the private sector perspective. Today, we hear from some of the agencies within our government that are working to meet these threats, both in terms of what is being done to promote cybersecurity as well as how we can better secure our nation's communications networks.

In this hearing, we are privileged to have five witnesses that represent parts of the government that work to address the complex cybersecurity issues our nation faces every day. The work being done by these government agencies to help address cybersecurity is just the tip of the iceberg of what we can achieve when our private sector innovation and public sector resources are put to a common task. That's why I am a co-sponsor of H.R. 3523, the Cyber Intelligence Sharing and Protection Act, a bi-partisan bill introduced by my Communications and Technology colleague and Chairman of the House Permanent Select Committee on Intelligence, Mike Rogers. H.R. 3523 makes commonsense changes to the way our government and the private sector share cyberintelligence without compromising either the commercial broadband providers or the integrity of the intelligence community. Similarly, the good work being done by industry stakeholders at the FCC on the Communications Security, Reliability and Interoperability Council – or CSRIC – to bring voluntary best practices to bear on the security of commercial networks is another example of the type of public-private cooperation that achieves results without mandates.

In addition to hearing from these agencies on the good work that they are doing, I also expect to hear how you think we can improve the cooperation between the federal government and private industry as they work to combat cyberthreats. Having heard from the private sector, today's public sector perspective will give the members of the subcommittee a more complete picture of the cybersecurity landscape.

I thank the panelists for their testimony today, and I look forward to a lively discussion of these issues.

###

Mr. WALDEN. With that, I would yield the remainder of my time to the gentleman from Nebraska, Mr. Terry.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Thank you, Mr. Chairman, and it is certainly quite a learning curve from both the Speaker's task force and the task force that Anna and I have been lucky enough to oversee.

But this is a real threat to our economy and to our country, and we need to really start thinking seriously about ways of securing our communications networks, and in that discussion, not only how but who should be part of that process, and first I want to commend the Communications Security and Reliability Interoperability Council, or CSRIC, for its recent report outlining voluntary best practices that industry has agreed to implement and ISPs engaging in the Anti-Bot Code of Conduct and Domain Name System best practices as well as working to develop a framework to prevent IP route hijacking is a great start to improving our overall health and safety of our Nation's networks and limiting access for attacks. I am confident that this collaboration will continue to improve.

I will state for the record that I have some reservations concerning giving government agencies like Department of Homeland Security authority for overseeing or implementing the standards. A, I think we need to focus on flexibility, and secondly, that department hasn't provided me the level of confidence that I would want to turn over our cybersecurity to them. All we have to do is walk into our airports and visualize my lack of confidence in them.

So at this point I will yield back, and I am anxious to hear from the witnesses.

Mr. WALDEN. I now recognize the gentlelady from California, my friend, Ms. Eshoo, for an opening statement.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman, and good morning to all of my colleagues on the subcommittee, and welcome to our witnesses. Thank you for being willing to be here today to instruct us even further on this whole issue of cybersecurity that we have had a very important series of hearings and they have been very, very helpful. They have been outstanding hearings, and both sides of the aisle, I think, have agreed on that.

As has been stated, I am part of the Cybersecurity Working Group with Congressman Terry, and through the process that we have followed, our collective staff have gathered information from key stakeholders and have been focusing on issues such as supply chain integrity, information sharing, consumer education, and it is obviously our subcommittee's jurisdiction in these areas. We have learned that Advanced Persistent Threats, the APTs, pose a significant risk to our communications infrastructure, and these sophisticated threats are often either state-sponsored or pursued by criminal enterprises and they have the potential to lead to significant theft or manipulation of data and other malicious activities.

So we have our hands full, most frankly, about how to go at this. Fortunately, there are experts like each one of you that are working hard, really diligently to protect our country from cyber threats, so we really look forward to hearing what you can instruct us on this, and I want to especially welcome Mr. Hutchinson from Sandia National Labs Adaptive Network Countermeasures—these are real mouthfuls, I will tell you—the ANC, the DHS efforts concerning domain name server security extension and the FCC's recent recommendations from CSRIC. All of these need to be stitched together. We can't afford to go into an enlightened endeavor and end up with silos all over again. I am very sensitive about that, having been a veteran of the House Intelligence Committee.

So I think to deter cyber criminals, we need to have a really well-coordinated, comprehensive effort that is going to promote R&D, consumer education, supply chain integrity and information and yet ensure at the same time that we speak to privacy and civil-liberties protections.

I think it is also important that we don't take any actions that would inadvertently hinder the private-sector development of cybersecurity technology or create new network vulnerabilities, and that is why I am pleased to see that both public and private sectors are working together on these issues and that the FCC's CSRIC unanimously endorsed voluntary industry-wide best practices to address the whole issue of botnets and domain name fraud and Internet route hijacking. So I think that they have done very good work and it is something that we need to take advantage of.

So today's hearing is really yet another opportunity for us to look at this slice that you can teach us about and that we weave that together all under the umbrella of really safeguarding some of the most important parts of our national infrastructure both public and private relative to cybersecurity.

Ms. ESHOO. With the time that I have remaining, I will yield it to Congresswoman Doris Matsui.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you very much, Ranking Member Eshoo, for yielding me time, and I would like to welcome our witnesses today, and I want to thank the chairman very much for having this hearing today and having explored some of these issues for the last month or so.

Communications networks are one of the many areas our Nation must protect to ensure safety and soundness. It will be important that data is protected in transit to cloud storage. A number of government agencies are using cloud services, so it is my hope that we can learn more from the early experiences.

I also believe that our subcommittee will have the ability to further promote information sharing on cyber threats. I will be interested in hearing from witnesses how information is being shared within the government and between the government and industry. There also seems to be a number of clearinghouses that are used to store information related to cyber threats. I will also be interested in hearing the relationship between those silos and industry and government sharing. Securing the supply chain will be of high importance.

We also need to consider that there might be some economic incentives that could encourage industry to explore ways to better address and defend against malware and botnets, and again, I welcome you all here today and I am looking forward to the testimony. Thank you very much.

Mr. WALDEN. Thank you, and thanks for your service on the working group.

Now I recognize Representative Bono Mack for a minute, and then we will have Mr. Barton and Ms. Blackburn.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mrs. BONO MACK. Thank you, Mr. Chairman.

In our two previous hearings on this issue, we have heard from representatives of the private sector and the communications industry who expressed real concern about the effects of heavy-handed new government regulation in this realm of cybersecurity. Onerous new regulations they say will likely fall haplessly behind existing technology and divert valuable resources away from security and towards regulatory compliance. Indeed, with so much information out there about the sophisticated and constantly evolving nature of cyber attacks, what the experts in the field have said they need most is the ability to better share information about existing cyber threats and the freedom to respond quickly to those threats.

Yesterday, Congresswoman Blackburn and I introduced the House companion to Senator John McCain's Secure IT Act, which first removes legal hurdles which prevent information sharing across the spectrum so that victims of cyber attacks can better work with each other to respond to cyber threats. I believe that this approach, which empowers security experts to proactively address threats rather than reactively respond to them, is the best path forward.

I look forward to hearing from our witnesses today. I thank them for appearing before us, and I would like to yield back the balance of my time.

Mr. WALDEN. And I would recognize the gentlelady from Tennessee for a minute.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I want to thank your witnesses for being here.

You have heard us talk about the two previous hearings that we have done with industry, and of course, what they have pointed out is that there is no cookie-cutter approach that we can follow as we deal with what are very dangerous issues. One of the things that also has come out is that the Federal Government needs to be leading by example. If we want to provide assurance that there is going to be a pattern of security, this is going to be important for us to do, to lead by example.

Another thing that as we discuss this and how we are going to lead by example, I also want to hear about what you are doing to prioritize your R&D and how we are going to be able to work with the private sector in that vein. As Representative Bono Mack introduced, we introduced the Secure IT Act yesterday. This is going to focus on strong info-sharing components, making certain that we are addressing some increased penalties for criminals and priority and coordination of the Federal research.

So thank you all, welcome, and yield back.

Mr. WALDEN. I now recognize Mr. Stearns for a minute.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Thank you, Mr. Chairman.

Yesterday, Shawn Henry, the FBI's top cyber cop, told the Wall Street Journal that the current public and private approach to fending off hackers is unsustainable as computer criminals are simply too talented and defensive measures are too weak to stop them. He also expressed that companies need to make major, major changes in the way they use computer networks to avoid further to national security, and Mr. Chairman, I ask that the Wall Street Journal article be part of the record by unanimous consent.

Mr. WALDEN. Without objection.

[The information follows:]

[redacted]

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | March 28, 2012, 10:31 a.m. ET

U.S. Outgunned in Hacker War

By DEVLIN BARRETT

WASHINGTON—The Federal Bureau of Investigation's top cyber cop offered a grim appraisal of the nation's efforts to keep computer hackers from plundering corporate data networks: "We're not winning," he said.

WSJ's Devlin Barrett reports the FBI is struggling to combat cyberattacks by hackers. "We're not winning," FBI executive assistant director Shawn Henry said. AP Photo/Haraz N. Ghanbari

Shawn Henry, who is preparing to leave the FBI after more than two decades with the bureau, said in an interview that the current public and private approach to fending off hackers is "unsustainable." Computer criminals are simply too talented and defensive measures too weak to stop them, he said.

His comments weren't directed at specific legislation but came as Congress considers two competing measures designed to buttress the networks for critical U.S. infrastructure, such as electrical-power plants and nuclear reactors. Though few cybersecurity experts disagree on the need for security improvements, business advocates have argued that the new regulations called for in one of the bills aren't likely to better protect computer networks.

Mr. Henry, who is leaving government to take a cybersecurity job with an undisclosed firm in Washington, said companies need to make major changes in the way they use computer networks to avoid further damage to national security and the economy. Too many companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking—or the costs they may have already suffered unknowingly—by operating vulnerable networks, he said.

Associated Press

'You never get ahead, never become secure, never have a reasonable expectation of privacy

"I don't see how we ever come out of this without changes in technology or changes in behavior, because with the status quo, it's an unsustainable model. Unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security," Mr. Henry said.

James A. Lewis, a senior fellow on cybersecurity at the Center for Strategic and International Studies, said that as gloomy as Mr. Henry's assessment may sound, "I am actually a little bit gloomier. I think we've lost the or security,' says Shawn Henry, executive assistant director of the FBI.

opening battle [with hackers]." Mr. Lewis said he didn't believe there was a single secure, unclassified computer network in the U.S.

"There's a kind of willful desire not to admit how bad things are, both in government and certainly in the private sector, so I could see how [Mr. Henry] would be frustrated," he added.

High-profile hacking victims have included Sony Corp., which said last year that hackers had accessed personal information on 24.6 million customers on one of its online game services as part of a broader attack on the company that compromised data on more than 100 million accounts. Nasdaq OMX Group Inc., which operates the Nasdaq Stock Market, also acknowledged last year that hackers had breached a part of its network called Directors Desk, a service for company boards to communicate and share documents. HBGary Federal, a cybersecurity firm, was infiltrated by the hacking collective called Anonymous, which stole tens of thousands of internal emails from the company.

Mr. Henry has played a key role in expanding the FBI's cybersecurity capabilities. In 2002, when the FBI reorganized to put more of its resources toward protecting computer networks, it handled nearly 1,500 hacking cases. Eight years later, that caseload had grown to more than 2,500.

Mr. Henry said FBI agents are increasingly coming across data stolen from companies whose executives had no idea their systems had been accessed.

"We have found their data in the middle of other investigations," he said. "They are shocked and, in many cases, they've been breached for many months, in some cases years, which means that an adversary had full visibility into everything occurring on that network, potentially."

Mr. Henry said that while many company executives recognize the severity of the problem, many others do not, and that has frustrated him. But even when companies build up their defenses, their systems are still penetrated, he said. "We've been playing defense for a long time. ...You can only build a fence so high, and what we've found is that the offense outpaces the defense, and the offense is better than the defense," he said.

Testimony Monday before a government commission assessing Chinese computer capabilities underscored the dangers. Richard Bejtlich, chief security officer at Mandiant, a computer-security company, said that in cases handled by his firm where intrusions were traced back to Chinese hackers, 94% of the targeted companies didn't realize they had been breached until someone else told them. The median number of days between the start of an intrusion and its detection was 416, or more than a year, he added.

In one such incident in 2010, a group of Chinese hackers breached the computer defenses of the U.S. Chamber of Commerce, a major business lobbying group, and gained access to everything stored on its systems, including information about its three million members, according to several people familiar with the matter.

In the congressional debate over cybersecurity legislation, the Chamber of Commerce has argued for a voluntary, non-regulatory approach to cybersecurity that would encourage more cooperation and information-sharing between government and business.

Matthew Eggers, a senior director at the Chamber, said the group "is urging policy makers to change the 'status quo' by rallying our efforts around a targeted and effective information-sharing bill that would get the support of multiple stakeholders and come equipped with ample protections for the business community."

The FBI's Mr. Henry said there are some things companies need to change to create more secure computer networks. He said their most valuable data should be kept off the network altogether. He cited the recent case of a hack on an unidentified company in which he said 10 years worth of research and development, valued at more than $1 billion, was stolen by hackers.

He added that companies need to do more than just react to intrusions. "In many cases, the skills of the adversaries are so substantial that they just leap right over the fence, and you don't ever hear an alarm go off," he said. Companies "need to be hunting inside the perimeter of their network," he added.

Companies also need to get their entire leadership, from the chief executive to the general counsel to the chief financial officer, involved in developing a cybersecurity strategy, Mr. Henry said. "If leadership doesn't say, 'This is important, let's sit down and come up with a plan right now in our organization; let's have a strategy,' then it's never going to happen, and that is a frustrating thing for me," he said.

Write to Devlin Barrett at devlin.barrett@wsj.com

Mr. STEARNS. Today's hearing focuses on public-sector responses to threats to communications networks. I am interested to hear our witnesses' reaction to Mr. Henry's bleak outlook on our unsustainable model to cybersecurity, as he says, "unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security."

As chairman of the Oversight and Investigations Subcommittee, I have held three cybersecurity hearings. Through these hearings and the ones held by our chairman today, I hope our committee can learn what we can do to make sure the good guys are winning again.

Thank you, Mr. Chairman.

Mr. WALDEN. I thank the gentleman from Florida. Is anybody else seeking recognition here? I know Mr. Barton had wanted time, but he is not here.

Now I will go to you, Mr. Waxman. We will return the balance of our time on this side and I now recognize the chairman emeritus, Mr. Waxman, for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Mr. Chairman, for holding this hearing on cybersecurity.

It is important that we understand the government perspective. I am especially interested to learn the steps government agencies are taking to advance cybersecurity and secure the supply chain. I also welcome our expert from Carnegie Mellon.

The FCC, under the leadership of Chairman Genachowski and Admiral Barnett, has established a Communications Security, Reliability and Interoperability Council, or CSRIC, and today we can learn about CSRIC's recent recommendations promoting cybersecurity, as well as what other agencies are doing to promote best practices and information sharing. Efforts like CSRIC can help lead to adoption of best practices and voluntary codes of conduct by Internet service providers, software companies, manufacturers and security vendors.

But we also need to address the question of accountability. For example, what if one company fails to be as diligent as others in following best practices and, as a result, causes a cyber breach that rises to the level of a national concern? We need to explore whether reliance solely upon the private sector to ensure the security of communications networks across the country is sufficient, and what additional steps we might need to achieve enough accountability to best protect critical communications networks from cyber attacks.

We are hearing from industry that they want statutory exemptions from privacy and antitrust laws in order to facilitate information sharing. I have an open mind as we consider these issues. But this should be a two-way street. If industry wants exemptions from consumer protection laws, we have a right to ask for accountability that companies actually end up sharing information important for cybersecurity, do not abuse their privileges, and are held accountable.

There is a stronger case to be made for enabling sharing between the Federal Government and private industry, but we need to balance information sharing with sufficient privacy and civil-liberties protections. Further, we need to make sure that the Federal agencies that engage in direct information sharing with the private sector are civilian agencies, not intelligence or defense agencies.

I hope we will also discuss securing the communications supply chain. This is a growing potential threat, especially as we are now witnessing thousands of applications being loaded onto smart devices that connect to the public Internet. We should examine the best ways to address this.

I want to thank our panel of witnesses for their participation today and I look forward to hearing your testimony. I yield back the time.

[The prepared statement of Mr. Waxman follows:]

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

Opening Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
Hearing on "Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
Subcommittee on Communications and Technology
March 28, 2012

Thank you, Mr. Chairman, for holding this hearing on cybersecurity. It is important that we understand the government perspective. I am especially interested to learn the steps government agencies are taking to advance cybersecurity and secure the supply chain. I also welcome our expert from Carnegie Mellon.

The FCC, under the leadership of Chairman Genachowski and Admiral Barnett, has established a Communications Security, Reliability and Interoperability Council, or "CSRIC". Today, we can learn about CSRIC's recent recommendations promoting cybersecurity, as well as what other agencies are doing to promote best practices and information sharing.

Efforts like CSRIC can help lead to adoption of best practices and voluntary codes of conduct by internet service providers, software companies, manufacturers, and security vendors. But we also need to address the question of accountability. For example, what if one company fails to be as diligent as others in following best practices and, as a result, causes a cyber breach that rises to the level of a national concern? We need to explore whether reliance solely upon the private sector to ensure the security of communications networks across the country is sufficient, and what additional steps we might need to achieve enough accountability to best protect critical communications networks from cyber attacks.

We are hearing from industry that they want statutory exemptions from privacy and antitrust laws in order to facilitate information sharing. I have an open mind as we consider these issues. But this should be a two-way street. If industry wants exemptions from consumer protection laws, we have a right to ask for accountability that companies actually end up sharing information important for cybersecurity, do not abuse their privileges, and are held accountable.

There is a stronger case to be made for enabling sharing between the federal government and private industry. But we need to balance information sharing with sufficient privacy and civil liberties protections.

Further, we need to make sure that the federal agencies that engage in direct information sharing with the private sector are civilian agencies, not intelligence or defense agencies.

I hope we will also discuss securing the communications supply chain. This is a growing potential threat, especially as we are now witnessing thousands of applications being loaded onto smart devices that connect to the public Internet. We should examine the best ways to address this.

Thank you to our panel of witnesses for your participation today. I look forward to hearing your testimony.

Mr. WALDEN. The gentleman yields back the balance of his time. We will now proceed with our witnesses. We thank you all for being here and look forward to your comments.

We will start with Ms. Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration, NTIA, U.S. Department of Commerce. That is a mouthful. We are glad you are here today and we look forward to hearing from you. And just a heads-up for everybody, these microphones, you have to get pretty close to for people to hear, and make sure it is lit.

STATEMENTS OF FIONA M. ALEXANDER, ASSOCIATE ADMINISTRATOR, OFFICE OF INTERNATIONAL AFFAIRS, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE; JAMES A. BARNETT, JR., CHIEF, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, FEDERAL COMMUNICATIONS COMMISSION; ROBERT L. HUTCHINSON, SENIOR MANAGER FOR INFORMATION SECURITY SCIENCES, SANDIA NATIONAL LABORATORIES; GREGORY E. SHANNON, CHIEF SCIENTIST, COMPUTER EMERGENCY READINESS TEAM, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY; AND ROBERTA STEMPFLEY, ACTING ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF FIONA M. ALEXANDER

Ms. ALEXANDER. Thank you very much. It is a very long name. So good morning, Chairman Walden, Ranking Member Eshoo and members of the subcommittee. Thank you for this opportunity to testify on behalf of the Department of Commerce's NTIA regarding cybersecurity.

NTIA, as you know, is the President's principal advisor on telecommunications and information policy matters and is the executive branch expert on issues relating to the Internet's Domain Name System, a critical component of the cyber infrastructure. NTIA supports a multi-stakeholder approach to the coordination of the DNS to ensure long-term viability of the Internet. Working with other stakeholders, NTIA develops policies and takes actions to preserve an open, interconnected global Internet that supports continued innovation and economic growth, investment and the trust of its users. This multi-stakeholder model of Internet policymaking convening the private sector, civil society and government to address issues in a timely and flexible manner, has been responsible for the past success of the Internet and is critical to its future.

The authenticity of DNS data is essential to the security of the Internet as it is vital that users reach their intended destinations and are not unknowingly redirected to fraudulent and malicious Web sites. This is one of the primary objectives motivating NTIA's efforts to secure the DNS and what I will specifically address today.

The early DNS, while exceptional in many ways, lacked strong security mechanisms. Over time, hackers and others have found more and more ways to exploit vulnerabilities in the DNS protocol.

That put the integrity of DNS data at risk. These vulnerabilities increase the likelihood of certain DNS-related cyber attacks which can lead to identify theft and other security compromises.

In response to these risks, the Internet Engineering Task Force developed a suite of specifications for securing information provided by the DNS called Domain Name System Security Extensions, or DNSSEC. DNSSEC provides an additional layer of security to DNS by authenticating the origin of the DNS data and verifying its integrity while it moves across the Internet.

In 2008, NTIA undertook a multi-stakeholder public consultation process regarding whether and how DNSSEC should be deployed at the authoritative route, the top level of a DNS hierarchy for which NTIA continues to have historical oversight. In response to the public notice, NTIA received overwhelming support from the international Internet community to move forward as soon as possible. Over the next year and a half, NTIA, drawing upon the input and expertise of technical experts from around the world, and working close with NIST, our sister agency at Commerce, as well as our root zone management partners, VeriSign and ICANN, moved to fully deploy DNSSEC at the root in July 2010.

DNSSEC essentially gives a tamper-proof seal to the address book of the Internet, similar to a wax seal on an envelope. For example, I can send you a letter in an envelope, but when you receive the envelope, you don't know if it was tampered with, but if I use my seal on some wax across the envelope's closure, then you know two things: the letter wasn't tampered with in transit, which means there is data integrity, and that I was the one who sent it, because you recognize my stamp, which is data origin authentication. If you know that I always seal my letters and you receive a letter from me that isn't sealed or the seal is broken, you know that a bad guy or a man in the middle could have opened the sealed envelope and replaced the contents. You can throw it away because you know it is a fake. DNSSEC information is like the letter in the envelope. DNSSEC gives that information a seal that verifies and authenticates it.

DNSSEC deployment at the authoritative root was an important step toward protecting the integrity of DNS data and mitigating attacks such as cache poisoning, which allows the hacker to redirect traffic to fraudulent sites and other data modification threats. This effort marks significant progress in making the Internet more robust and secure as it provides a tool to facilitate greater user confidence in the online experience so that when someone visits a particular Web site, whether it be a bank, a retailer or a doctor, they are not seeing a spoofed copy that cyber criminals can use to perpetuate identify theft or other crimes using the DNS.

In helping to deploy DNSSEC at the root zone, NTIA sought to facilitate greater DNSSEC deployment throughout the Internet. If we are to maintain trust in the Internet, then we must support further DNSSEC deployment. Governments as well as other stakeholders must continue to support the deployment and development of DNSSEC-related software, tools and other products and services. As we explore issues affecting Internet space, we should take all appropriate steps to ensure that DNSSEC use and adoption continues to grow.

In the coming months, NTIA, working as a part of the Department of Commerce's Internet Policy Task Force, will be looking for opportunities to launch further multi-stakeholder processes aimed at enhancing the security and stability of the DNS as well as broader cybersecurity efforts.

Thank you again for the opportunity to testify, and I will be happy to answer any questions.

[The prepared statement of Ms. Alexander follows:]

Testimony of Fiona M. Alexander
Associate Administrator, Office of International Affairs
National Telecommunications and Information Administration
United States Department of Commerce

Before the

Committee on Energy and Commerce
Subcommittee on Communications and Technology
United States House of Representatives

Hearing on
"Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
March 28, 2012

Introduction

Good morning Chairman Walden, Ranking Member Eshoo, and Members of the Committee. Thank you for this opportunity to testify on behalf of the Department of Commerce's National Telecommunications and Information Administration (NTIA) regarding cybersecurity. NTIA is the President's principal advisor on telecommunications and information policy matters, and is the Executive Branch expert on issues relating to the Internet's domain name system (DNS) - a critical component of the cyber infrastructure. NTIA supports a multi-stakeholder approach to the coordination of the DNS to ensure the long-term viability of the Internet as a force for innovation and economic growth. Working with other stakeholders, NTIA develops policies and takes actions to preserve an open, interconnected global Internet that supports continued innovation and economic growth, investment, and the trust of its users. This multi-stakeholder model of Internet policymaking – convening the private sector, civil society, as well as governments to address issues in a timely and flexible manner – has been responsible for the past success of the Internet and is critical to its future.

The Internet plays an increasingly vital role in daily life, from helping businesses expand to improving education and health care. Every day, millions of Americans shop, sell, bank, learn, talk, and work online. At the turn of the century, online retail sales totaled approximately $20 billion in the United States, now they are nearing $200 billion. The growth of the Internet is due in part to the trust of its users – trust, for example, that when users type a website address, they will be directed to their intended destination. Given the Internet's importance to the Nation's economic and social advancement, it is essential that the Internet - and its underlying infrastructure - remain stable and secure. This is a primary objective motivating NTIA's efforts to secure the DNS and what I specifically will address today.

DNS Vulnerabilities and Efforts to Enhance Security through DNSSEC

The DNS is a critical component of the Internet infrastructure. It works like a telephone directory, allowing users to reach websites using easy-to-understand domain names (e.g., http://www.commerce.gov) rather than the numeric network server addresses (e.g., http://170.110.225.194) necessary to retrieve information on the Internet. The authenticity of the DNS data is essential to the security of the Internet – it is vital that users reach their intended destinations on the Internet and are not unknowingly redirected to fraudulent and malicious websites.

The early DNS, while exceptional in many ways, lacked strong security mechanisms. Over time, hackers and others have found more and more ways to exploit vulnerabilities in the DNS protocol that put the integrity of DNS data at risk. These vulnerabilities increase the likelihood of certain DNS-related cyber attacks, such as man-in-the-middle attacks, which could lead to identity theft and other security compromises.

In response to these risks, the Internet Engineering Task Force (IETF), a multi-stakeholder body that develops and promotes Internet standards, developed Domain Name System Security Extensions (DNSSEC), a suite of specifications for securing information provided by the DNS. DNSSEC provides an additional layer of security to the DNS by authenticating the origin of DNS data and verifying its integrity while it moves across the Internet.

NTIA's Efforts to Promote DNSSEC

In 2008, NTIA undertook a multi-stakeholder public consultation process regarding whether and how DNSSEC should be deployed at the authoritative root of the DNS – the top-level zone of the DNS hierarchy for which NTIA has historical oversight.[1] In response to the public notice, NTIA received an overwhelming response from the global multi-stakeholder Internet community supporting efforts to implement DNSSEC at the authoritative root as soon as possible. Over the next year and a half, NTIA worked closely with the Department of Commerce's National Institute of Standards and Technology (NIST), as well as its root zone management partners – VeriSign and the Internet Corporation for Assigned Names and Numbers (ICANN) – to fully deploy DNSSEC at the root in July 2010. This effort enjoyed the support of the multi-stakeholder Internet community and drew upon the input and expertise of technical experts from around the world.

DNSSEC deployment at the authoritative root was an important step toward protecting the integrity of DNS data and mitigating attacks such as cache poisoning, which allows an attacker to redirect traffic to fraudulent sites, and other data modification threats. This effort marked significant progress in making the Internet more robust and secure. DNSSEC essentially

[1] For more information, see http://www.ntia.doc.gov/legacy/DNS/noi_10092008.html.

gives a "tamper proof seal" to the address book of the Internet, and in so doing, gives Internet users greater confidence in their online experience. As a result, Internet users will have greater confidence that when they visit a particular website – whether it be their bank, retailer, or doctor – they are not seeing a spoofed copy that cybercriminals can use to perpetuate identity theft or other crimes using the DNS.

In helping to deploy DNSSEC at the root zone, NTIA sought to facilitate greater DNSSEC deployment throughout the rest of the global DNS hierarchy. To realize the greatest benefits of DNSSEC, there needs to be broad deployment, support, and participation of actors throughout the Internet landscape, including, for example, domain name registrars, top-level domain registry operators, ISPs, software vendors, and others. Since the deployment of DNSSEC at the root, adoption of DNSSEC has increased throughout the Internet ecosystem. While these efforts are encouraging, NTIA is committed to increasing adoption further.

If we are to maintain trust in the Internet, we must support further DNSSEC deployment. Governments, as well as other stakeholders, must continue to support the deployment and development of DNSSEC-related software, tools, and other products and services. As we explore issues affecting the Internet space, we should take all appropriate steps to ensure that DNSSEC use and adoption continues to grow and to maintain the security and stability of the DNS. In the coming months, NTIA, working as a part of the Department's Internet Policy Task Force, will be looking for opportunities to launch further multistakeholder processes aimed at enhancing security and stability of the DNS as well as broader cybersecurity efforts.

Conclusion

Thank you again for the opportunity to testify. NTIA looks forward to working with Congress, U.S. business, individuals, and other stakeholders to preserve and enhance the security and stability of the Internet DNS. NTIA will continue its efforts to support the broader deployment of DNSSEC and welcomes the opportunity to continue this discussion in the future.

I will be happy to answer any questions.

Mr. WALDEN. Ms. Alexander, we appreciate your comments and we look forward to the questions.

Admiral, we are delighted to have you here today, Admiral James Barnett, Jr., Retired, Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission, the FCC. Welcome, and we look forward to your comments.

STATEMENT OF JAMES A. BARNETT, JR.

Mr. BARNETT. Thank you, Chairman Walden, Ranking Member Eshoo and all the distinguished members of the subcommittee. I really appreciate the opportunity to come and talk to you on this important topic of cybersecurity, and I am particularly pleased to be able to testify with these experts and especially my colleagues from DHS and Commerce with whom we work very closely on cybersecurity matters.

Cybersecurity threats are a real and present danger to our current economy and wellbeing. No one would tolerate the level of criminality, thievery, vandalism or invasion of privacy that we experience today if it were done in the physical world, and we really can no longer afford to tolerate it in cyber space.

The approximately 40,000 autonomous systems or networks on which the Internet is built are largely commercial or privately owned. Commercial communications providers are therefore the first line of defense against cyber threats and always will be. Earlier this month, on March 7th, the subcommittee heard from cybersecurity experts in the communication industry about how hard they are working against those threats, yet if those efforts alone were sufficient to thwart cyber threats, I don't think we would be here today. To be successful in battling cyber threats, we must work together collectively, industry and the public sector.

As the Nation's expert agency on communications, we have always been concerned with the security and reliability of networks. The FCC has a long history of working on network reliability and security with the companies that operate the core of the Internet. We have constituted a Cybersecurity and Communications Reliability Division in the Public Safety and Homeland Security Bureau. These are our cyber experts who among other duties coordinate the work of our current Federal advisory committee, the Communications Security, Reliability and Interoperability Council, CSRIC which you mentioned before. CSRIC is now made up of over 50 industry leaders from the private sector and the Federal Government including cyber experts from DHS and NIST and a veritable all-star cast of Internet pioneers and world-class cybersecurity experts that are working on the council and the working groups.

And I am pleased to report that last week, CSRIC approved voluntary industry-based recommendations addressing three crucial problems. These recommendations are not simply a set of reports that will adorn bookshelves. Numerous ISPs including Comcast, Verizon, AT&T, Time Warner, Sprint, Cox, T–Mobile, Frontier and CenturyLink have already pledged to implement the CSRIC recommendations as they apply to their respective networks. This means that these new cybersecurity measures will soon be protecting a significant majority of American Internet users.

First, CSRIC recommended that ISPs adopt a voluntary code of conduct to provide critical security to Internet users to fight botnets, which can steal personal information. We refer to it as the anti-bot code, a code that specifically addresses privacy of the end user.

Second, CSRIC examined Internet route hijacking, which can occur due to the lack of verification between networks. Internet route hijacking can endanger valuable intellectual and private property and jeopardize our national security. In 2010, traffic to 15 percent of the world's Internet destinations was diverted through Chinese servers for approximately 18 minutes. CSRIC recommended that ISPs embark upon a path toward implementation of secure routing protocols, or secure BGP, to minimize route hijacking. This would include the establishment of a secure, authoritative database of Internet address blocks to be used and checked by ISPs

CSRIC's third area of action is the Domain Name System, DNS, which Ms. Alexander just mentioned. DNS can be thought of as the telephone book for the Internet, one that can be spoofed and can lure exposure of private information. DNSSEC can correct this problem. It was designed with privacy in mind. CSRIC endorsed DNSSEC implementation by ISPs and industry-wide adoption of the standard to help prevent unsuspecting Internet users from being sent to fraudulent Web sites.

These voluntary initiatives stand as an example to the world of how to promote cybersecurity while preserving the core characteristics of the Internet, which have fueled the broadband economy's growth and success. These efforts focus on ISPs but they dovetail into broader cybersecurity efforts by NIST and DHS which must address the larger information technology community. We will continue to work with industry, the multi-stakeholders and Federal partners on voluntary industry-based solutions. We will carefully guard the reliability and security of all communications networks. Thank you.

[The prepared statement of Mr. Barnett follows:]

Testimony of
James Arden Barnett, Jr.
Rear Admiral, USN (Retired)
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Before the
Subcommittee on Communications, Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives

Hearing on "Cybersecurity: Threats to Communications Networks and Public-Sector Responses"

March 28, 2012

Good morning, Chairman Walden, Ranking Member Eshoo, and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the important topic of cybersecurity threats to communications networks. The Federal Communications Commission has been working with a broad cross-section of the broadband economy; world-class engineers who helped invent and develop the Internet and who understand the latest technologies and trends; award-winning academics; and dedicated federal partners from across government to address the threat posed by cyber attacks.

As you are all aware, cyber attacks present a critical threat to our economic future. More than $8 trillion dollars flow over these networks each year and that amount is growing. Approximately 150 million Americans shop or bank online.[1] And more than 1 million entrepreneurs rely on these networks for the life blood of their businesses.

Beyond commerce, these networks are driving breakthroughs in health care, education, energy, manufacturing, public safety, and other sectors of the economy, as well as providing a forum for free speech and expression of which our founding fathers would be proud. Simply put these networks have transformed the way we connect and communicate with one another and they have transformed every sector of our economy and the world economy.

The benefits of this transformation however do not come without security risks for consumers, businesses, and government.

[1] *See* http://www.emarketer.com/blog/index.php/tag/how-many-people-shop-online/

For example, in April 2011, a massive cyber-attack on Sony's PlayStation Network and Qriocity services led to the compromise of 77 million user accounts. In hacking the Japanese company's database, thieves made off with personally identifiable user information, including dates of birth, e-mail and home addresses and login credentials.[2] Millions of Americans are unaware that their home or office computers have been infected and are being controlled remotely by cyber criminals, so called botnets, that send spam or secretly attack the websites of businesses, not-for-profits, and government agencies. Citigroup is one of several high-profile companies that suffered a cyber-attack. In June of 2011, the bank reported that 210,000 of its card holders had their personal data compromised by hackers. The stolen information included names, account numbers and e-mail addresses.[3]

In May, Fidelity National Information Services reported that profits experienced a $13 million loss due to "unauthorized activities." A group of criminals hacked the company's network and gained access to its central database where card balances are kept. The criminals then obtained 22 legitimate prepaid cards, and made copies that were shipped to conspirators in Greece, Russia, Spain, Sweden, Ukraine and the United Kingdom. The crooks were able to increase the balances of the cards, making it possible for their worldwide criminal partners to withdraw cash from dozens of ATMs during a 24-hour period.[4]

The Ponemon Institute found that the median annualized cost of cyber crime for the 50 organizations in their study was $5.9 million, with the range being $1.5 million to $36.5 million.[5] According to a Symantec survey, three-quarters of small and medium businesses report being affected by cyber attacks.[6]

No one would tolerate this level of criminality, thievery, vandalism, or invasion of property if it was done in the physical world, and we can no longer afford to tolerate it in cyberspace.

Private Industry's Response

Luckily, the United States has the resources to respond to these threats. The approximately 40,000 autonomous systems or networks on which the Internet is built are largely commercial or privately owned, and connected on the basis of trust, a basis that is increasingly vulnerable.. The

[2] *See* http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=11

[3] *See* http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=9

[4] *See* http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=10

[5] *See* http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

[6] *See* http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf?om_ext_cid=biz_socmed_twitter_2010Jun_worldwide_SMB *at* 3.

commercial communications providers are therefore the first line of defense against cyber threats and always will be.

I have had the opportunity to visit some of their operations centers, and on a minute-by-minute basis, around the clock, these providers ably and vigorously defend their networks from constant attacks. I am very impressed with the level of expertise and dedication that these commercial providers exert to protect against these cyber attacks. Earlier this month, on March 7, this subcommittee heard from cybersecurity experts in the communications industry about how hard they are working against those threats and those attacks.

Yet, if their efforts alone were sufficient to thwart cyber threats, we would not be here today. To be successful in battling cyber threats, we must work together, collectively, private industry and the public sector.

So your line of inquiry on the proper and effective roles of government and its agencies is salient.

Principles of Government Action in Cybersecurity

In pursuing the proper roles of government in cybersecurity, we must observe some key principles:

1. We must ensure that the broadband economy remains an engine of innovation and growth, increasingly available to and used by Americans.
2. Sacrificing privacy or Internet openness for security is a false choice. We must insist on having all three, and we strongly believe that this is achievable.
3. We must preserve the multi-stakeholder model to tackle Internet issues like cybersecurity. Stakeholders across the ecosystem will need to work together and develop practical solutions to secure our networks.
4. We should seek smart, practical, voluntary solutions through cooperative efforts to achieve cybersecurity, whenever it is possible and effective.
5. Federal partners must work closely together in a whole-of-government approach. We must bring all our talent and efforts to bear and cannot afford to leave talent on the sidelines or pursue uncoordinated actions.

I will return to these principles later in my testimony, but with them in mind, I will turn to the FCC's role and actions in cybersecurity.

The FCC's Role and Actions in Cybersecurity

The FCC was established by Congress for the purpose of national defense and to promote the safety of life and property through the use of wire and radio communications. As the nation's expert agency on communications, we have always been concerned with the security and reliability of networks. The FCC has a long history of working on network reliability and security with the companies that operate the core of the Internet. In the spirit of seeking non-regulatory answers first, we have a longstanding practice of working collaboratively with industry, federal partners, public safety, and others to enhance network reliability and security. We have had success as a convener and facilitator of the communications industry. As long ago as 2001, the FCC's industry-based advisory committee, the Network Reliability and Interoperability Council (NRIC) delivered the first set of cybersecurity best practices anywhere in the federal government.

After I arrived at the FCC in 2009, I proposed the reorganization of one of our Public Safety and Homeland Security Bureau's divisions into the Cybersecurity and Communications Reliability Division (with the approval of Congress) and continued to add cybersecurity and communications experts to augment our capability. This division helps coordinate the work of our current federal advisory committee, which succeeded the NRIC, the Communications Security, Reliability and Interoperability Council (CSRIC)

The CSRIC is now made up of over 50 industry leaders from the private sector, engineers, and the federal government, including cyber experts from DHS and NIST and a veritable all-star cast of Internet pioneers and world class cybersecurity experts.

In March 2011, Chairman Genachowski tasked the CSRIC with developing best practices to help address major Internet security vulnerabilities. The Chairman identified three areas where action is required to better protect commercial communications networks:

1. Securing the Doman Name System (DNS) to prevent spoofing and DNS cache poisoning (DNS is like the plain language telephone book for the World Wide Web to help you find where you want to go);
2. Improving the security of Border Gateway Protocols to prevent Internet route hijacking; and
3. Defeating botnets which cause distributed denial of service attacks and pilfer private information and money.

I am pleased to report that last week the CSRIC approved voluntary, industry-based recommendations addressing all three critical problems. Moreover, these recommendations are not simply a set of reports that will adorn bookshelves. Numerous ISPs, including Comcast, Verizon, AT&T, Time Warner, Sprint, Cox, T-Mobile, Frontier and Century Link have already pledged to implement the CSRIC recommendations as they apply to their respective networks and infrastructure. This means that these new cybersecurity measures will soon be protecting a significant majority of American Internet users, and we hope more ISPs will adopt these measures.

I would like to briefly describe the three network threats and vulnerabilities on which we have focused.

First, CSRIC recommended that ISPs adopt a voluntary Code of Conduct to provide a critical baseline framework of security to all Internet users to mitigate the botnet threat, which we refer to at the Anti-Bot Code. The Anti-Bot Code encourages ISPs to participate in activities in support of:

1. End-user education to prevent bot infections;
2. Detection of bots;
3. Notification of potential bot infections;
4. Remediation of bots; and
5. Collaboration and sharing of information from participating in the Code.

Of course, ISPs can and must do this in a way that does not compromise consumers' privacy. In fact, respect for privacy is a core implementation principle of the Anti-Bot Code. As such, all ISPs who volunteer to participate in the Code must agree to adhere to applicable privacy laws affecting the execution of their bot and botnet education, detection, notification, remediation, and collaboration activities. By doing so, these voluntary actions help protect the privacy of American consumers and businesses from those who would seek to steal identities, money, and property.

Industry leaders Comcast, CenturyLink and others have already implemented these measures, and as I mentioned, many other ISPs representing millions of American users signed on last week. This will not end botnets, but when fully implemented, this will make it significantly harder for bad actors to operate botnets.

The second major security challenge examined by the CSRIC is Internet route hijacking.

The autonomous networks upon which the Internet is built rely on an implicit trust that is the Internet's greatest strength, but can also be a major weakness. The protocol that enables seamless connectivity among these networks, known as Border Gateway Protocol or BGP, does not have built-in mechanisms to protect against cyber attacks. This makes it possible for bad actors to misdirect Internet traffic meant for one destination through the hands of another network.

During the time the traffic is diverted, the network through which it has been diverted can "eavesdrop" on the information passing through, stealing or changing the information before it arrives at its intended destination. Internet route hijacking can endanger valuable intellectual property, other personal property, and jeopardize our National security. In 2010, traffic to 15 percent of the world's Internet destinations was diverted through Chinese servers for approximately 18 minutes.[7] According to numerous media reports, in 2008, traffic intended for YouTube was misrouted for about two hours due to the actions of a Pakistani Internet service provider.[8] Misrouted traffic, whether intentional or accidental, is clearly unacceptable.

The CSRIC recommended ISPs develop a path toward the implementation of secure routing protocols and best practices to minimize the likelihood and impact of BGP exploits. In particular, it recommended:

[7] http://www.reuters.com/article/2010/11/19/us-china-internet-idUSTRE6AI1DK20101119

[8] Pakistan's YouTube Blockage Caused Outage. John Ribeiro, February 25, 2008.

http://abcnews.go.com/Technology/PCWorld/story?id=4339294

1. The establishment of a touchstone of ground truth, in essence, a secure, authoritative database of Internet address blocks to be used and checked by ISPs. This would be an Internet registry established by industry, not government and in fact, the American Registry of Internet Numbers (ARIN) has already volunteered to establish the registry. This is appropriate, since ARIN actually assigns IP address blocks to ISPs now;
2. The registration and maintenance of ISP address blocks in the authoritative registry; and
3. The phased deployment of techniques that detect and prevent route hijacking by checking routes against the registry. Each network would still retain the local autonomy to decide how to store, disseminate, and utilize the certified number resources information and how to route.

CSRIC also recommended better metrics and continuous monitoring to quantify the frequency and scope of routing system security incidents and to evaluate the effectiveness of proposed security improvements, particularly those related to inter-domain routing on the Internet. More work will be needed to completely secure Internet routing through a secure BGP, and some of those standards and equipment are a few years off. However, the benefits of ISPs taking these steps now to help eliminate misrouted traffic will be momentous.

Our third area of action is the Domain Name System (DNS). DNS can be thought of as the telephone book for the Internet; DNS servers are filled with identifying information for web sites, which is used to direct Internet users to websites they want to visit. The Domain Name System provides a simple and convenient way to associate and translate easily remembered names, known as domain names (for example, www.fcc.gov), to numerical IP addresses (for example, 201.96.10.10) that are used to find Internet sites.

Domain name fraud occurs when bad actors change the identifying information, so that an unsuspecting Internet user attempting to go to one website can be misdirected to another website, oftentimes a fraudulent one. The fake website may be designed to look exactly like the real one so that the user can be tricked into providing their financial and personal information.

For instance, in 2009 the customers of one of Brazil's biggest banks were the victims of DNS fraud. They found themselves on a fake website that looked exactly like the bank's real one. Customers' user names and passwords were stolen for four hours until the crime was discovered.[9]

A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.[10]

The good news is that the Internet Engineering Task Force (IETF), an organization that develops and promotes Internet standards, has developed a solution to the vulnerabilities in the Domain Name System, Domain Name System Security Extensions or DNSSEC. The extensions are an

[9] http://cyberinsecure.com/cache-poisoning-attack-sends-top-brazilian-bank-users-to-scam-sites/

[10] http://www.gartner.com/it/page.jsp?id=565125

add-on to the DNS protocol and are being used by several large ISPs and government agencies.

Since the original design of DNSSEC, measures have been taken to ensure that it functions in a way that is consistent with privacy laws. As such, DNSSEC was designed with privacy in mind and it can and must be implemented in a way that protects individual privacy. The CSRIC endorsed ISPs embarking on DNSSEC implementation, and Chairman Genachowski called for industry-wide adoption of the standard to help prevent unsuspecting Internet users being sent to fraudulent websites.

These three initiatives have been developed consistent with the principles that I stated earlier. They have been developed using a multi-stakeholder, voluntary approach. These initiatives are in keeping with Organization for Economic Cooperation and Development's principles for Internet policymaking, which emphasize the importance of multi-stakeholder cooperation to promote network security, and were endorsed by the United States and 34 other countries.[11] They are non-regulatory, industry-based and have been worked on in cooperation with our federal partners. These initiatives fit under the aegis of broader cybersecurity efforts being led by the Department of Commerce, the National Institute of Standards and Technology (NIST) and the Department of Homeland Security. They are common travelers with the National Strategy for Trusted Identities in Cyberspace (NSTIC). They stand as an example to the world of how to promote cybersecurity while preserving the core characteristics of the Internet that have fueled the broadband economy's growth and success.

CSRIC's work will be ongoing because bad actors will continue to try to innovate around our defenses and measures. We must out-innovate them.

In closing, I am proud of the actions that have been taken just last week on the Botnet Code of Conduct and implementation practices for securing Internet routing and the Domain Name System. The FCC will remain focused on cybersecurity threats to communications networks. We will continue to work with a wide range of stakeholders, including industry and federal partners on voluntary, industry-based solutions. We will carefully guard the reliability and security of all communications networks. Thank you.

[11] White House Technology website, http://www.whitehouse.gov/issues/technology#id-1

Mr. WALDEN. Admiral, thank you very much. We appreciate your testimony, even if it is ever more disturbing the more we hear.

With that, we will now go to Mr. Hutchinson, Senior Manager for Information Security Sciences at Sandia National Laboratories. Thanks for all the work you and your team do out there at Sandia, and we appreciate your being here today to further enlighten us about the threat that we face and how we might deal with it appropriately, so please go ahead.

STATEMENT OF ROBERT L. HUTCHINSON

Mr. HUTCHINSON. Good morning. Chairman Walden and Ranking Member Eshoo and the distinguished members of the committee, thank you for inviting me to testify before you today. I am Bob Hutchinson, Senior Manager for Information Security Sciences at Sandia National Laboratories. Sandia is a federally funded research and development center for the Department of Energy. DOE makes its significant investment in Sandia's cybersecurity capabilities available to the Departments of Defense and Homeland Security as well as other government agencies and non-Federal entities.

I have been working to secure critical government communications systems both as a researcher and as an implementer for over 25 years, and today's testimony is based on that experience. The most important lesson that I have learned in my career is that computer systems can never be fully trusted and can never be proven free of compromise, so we must focus on finding ways to conduct business, even critical business, on machines that are presumed to be infected. Our focus should be on accomplishing our goals and not on building and maintaining perfect computers and computer networks.

I would like to suggest four specific shifts in current national approach to cybersecurity. Each of these suggestions implies a role for the government and a role for the private sector. My intention is to highlight the strengths of each of these communities and to find ways that they can reinforce each other's interests.

Number one: In recent years, the Nation's cybersecurity approach has shifted to an almost exclusive focus on data theft. While this trend has been going for a number of years it understandably worsened in the aftermath of the Wikileaks intelligence theft. Our best security analysts are being taught to focus their attention on indications that sensitive data is leaving our networks headed into enemy hands. While data theft is a critical problem for the government and for the private sector, I believe that our Nation has diverted too many resources away from an equally, if not more important issue: malicious data modification. As much as I worry about the theft of sensitive data and U.S. intellectual property, my greater fear is that an attacker will alter our data and affect our decision processes. This form of attack has not only economic consequences but can also impact public safety and confidence. My staff and I focus much of our research on these scenarios. The security community must continue to worry about data theft but not to the detriment of other cyber attack goals. The government should increase focused research and development investment on preserving data integrity.

Number two: We tend to view the stacks of mobile devices and networking components that arrive in U.S. ports as pristine. When we discover a compromise, we strive to return these devices to their original settings. This is a fundamentally flawed security model. We don't have any idea whether our devices have been precompromised during design, manufacture or distribution. We call this a supply chain attack. As an unclassified example, a few years ago a major hard-drive manufacturer was discovered to have shipped brand-new hard drives with malware preinstalled. The government, in part through Sandia, has been addressing these supply chain attacks for over three decades. The commercial companies share this risk with the government. The government can help industry by informing commercial companies of our lessons learned and helping those companies use their existing supply relationship to begin addressing this problem where it will have the greatest impact directly within the company's own supply chains.

Number three: It is not enough that the government shares details of cybersecurity incidents with the community of interest. It also needs to develop and share strategies. Cybersecurity is more like a game of poker than a reaction not a natural disaster. Simply sharing data without rules and strategies prevents us from working together effectively. For instance, careful coordination of our activities can cause an adversary to reveal his identity.

Finally, number four: The most consistent cybersecurity message across government and industry is that our Nation has a profound shortage of qualified cybersecurity experts. There are many efforts to educate, train and certify. Degrees and certifications are not enough. Cybersecurity is a new field that lacks scientific and engineering rigor. The best people in this field learn through practice and apprenticeship. They use judgment that is based on years of experience. The Department of Energy began to address this issue over 10 years ago when they asked Sandia to build a program that is more like a medical residency than a trade certification. Many of the people who have participated in this program have become national leaders in securing emerging technologies such as mobile device networks and cloud services. This investment has yielded greater returns than any other program in which I have been involved. Expanding this model so that all U.S. cybersecurity professionals learn through a residency would result in enormous gains for national security.

I would like to thank you for this opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Hutchinson follows:]

Statement of Robert L. Hutchinson
Senior Manager for Information Security Sciences
Sandia National Laboratories

United States House of Representatives Committee on Energy and Commerce
Subcommittee on Communications and Technology

March 28, 2012

Chairman Walden and Ranking Member Eshoo, and the distinguished members of the Committee; thank you for inviting me to testify before you today. I am Bob Hutchinson, Senior Manager for Information Security Sciences at Sandia National Laboratories.

Sandia is a multi-program, multi-disciplinary Department of Energy national laboratory operated by Sandia Corporation as a Federally Funded Research and Development Center. We are an independent entity sponsored by the U.S. government to provide detailed technical expertise on complex national challenges.

Sandia has over fifty years of experience protecting critical information systems against sophisticated adversaries. The Department of Energy makes its significant investment in Sandia's cyber security capabilities available to the Departments of Defense and Homeland Security, as well as other government agencies and non-federal entities. A key element of our work is to help increase the overall cyber security of public and private communications networks. Further, Sandia often functions as a hub that works at the intersection of academia, industry, and government to drive cyber innovation and advance the overall national and global cyber health.

I've been working to secure critical government computer systems—both as a researcher and as an implementer—for over 25 years, and today's testimony is based on that experience.

The most important lesson I have learned in my career is that computer systems can never be fully trusted, can never be proven free of compromise, so we must focus on finding ways to conduct business, even critical business, on machines that are presumed to be infected. We can all be victimized by countless threats in our daily lives—car accidents, diseases, theft—and yet we have found ways to manage those daily risks and move about our days. This mindset has served us well for centuries and must be applied to computer security; our focus should be on accomplishing our goals not on building and maintaining perfect computers and networks.

I would like to suggest four specific shifts in the current national approach to cyber security. Each of these suggestions implies a role for the government and a role for industry. My intention is to highlight the strengths of each of these communities and to find ways that they can reinforce each other's interests.

Number one: In recent years, the nation's cyber security approach has shifted to an almost exclusive focus on data theft. While this trend has been growing for a number of years, it understandably worsened in the aftermath of the Wikileaks intelligence theft. Our best security analysts are being taught to focus their attention on indications that sensitive data is leaving our networks, headed into enemy hands. While data theft is a critical problem for government and for industry, I believe that our nation has diverted too many resources away from an equally, if not more, important issue: malicious data modification. As much as I worry about the theft of sensitive government data and US intellectual property, my greater fear is that an attacker will alter our data and affect our decision processes; this form of attack has not only economic consequences, but can also impact public safety and confidence. My staff and I focus much of our research on these scenarios. We must continue to worry about data theft, but not to the detriment of other cyber attack goals. The government should increase focused research and development investment on preserving data integrity.

Number two: We tend to view the stacks of mobile devices and networking components that arrive at US ports as pristine; when we discover a compromise, we strive to return devices to factory original settings. This is a fundamentally flawed security model. We don't have any idea whether our devices have been pre-compromised during design, manufacture, or distribution; we call this a supply chain attack. As an unclassified example, a few years ago, a major hard drive manufacturer was discovered to have shipped brand new hard drives with malware pre-installed. The government, in part through Sandia, has been addressing these supply chain attacks for over three decades. But commercial companies share this risk with the government. The government can help industry by informing commercial companies of our lessons learned, and helping those companies use their existing supplier relationships to begin addressing this problem where it will have the greatest impact: directly within the companies' own supply chains.

Number three: The government is taking significant steps in sharing information about cyber threats with industry; what makes this task difficult is a lack of agreement on what should be done with the shared data. We need information sharing that enables a community of stakeholders to execute a strategy. For example, can we cause an adversary to reveal his identity? Before we can achieve this goal, we need information sharing systems that respect not only data, but the strategy and rules associated with that data. A system with clear, enforced rules should enable both government and industry to benefit while allowing all stakeholders to effectively manage their own business interests and risks.

Finally, number four: The most consistent cyber security message across government and industry is that our nation has a profound shortage of qualified cyber security experts. There are many efforts to educate, train, and certify. Degrees and certifications are not enough. Cyber security is a new field of study that lacks science and engineering rigor. The best people in this field learned through practice and apprenticeship; they use judgment that is based on years of experience. The Department of Energy made this discovery over ten years ago, when they asked Sandia to build a program that's more like a medical residency than a trade certification. Many of the people who have participated in this program have become national leaders in securing emerging technologies such as mobile device networks and cloud services. This investment has yielded greater returns than any other program that I've been involved in. Expanding this model so that all US cyber security professionals learn through a form of residency would result in enormous gains for national security.

Thank you for the opportunity to testify; I look forward to your questions.

Mr. WALDEN. Thank you, Mr. Hutchinson. We appreciate your disturbing testimony.

Now we are going to go to Mr. Greg Shannon, the Chief Scientist, Computer Emergency Readiness Team, Software Engineering Institute at Carnegie Mellon University. Dr. Shannon, thank you for being here. We look forward to your testimony.

STATEMENT OF GREGORY E. SHANNON

Mr. SHANNON. Thank you, Chairman Walden, Ranking Member Eshoo and distinguished committee members. I am honored to testify before you today on cybersecurity and communication networks. I am the Chief Scientist for the CERT cybersecurity program at the Software Engineering Institute, which is a Department of Defense FFRDC operated by Carnegie Mellon University.

CERT was created in 1988 by DARPA in response to the moratorium incident and now we are a national asset for cybersecurity with 250 staff tackling our Nation's technical cybersecurity challenges. At CERT, we recognize the long-term challenges as we confront the threats, deliver pragmatic solutions and consider the technical roles for the private and public sectors. We see two important policy opportunities with long-term benefits.

First is to broadly promote the use of scientifically and operationally validated policies, best practices, technologies, standards, products, etc. Validated capabilities should trump unvalidated ones.

Second is to actively enable controlled access to real high-fidelity operational data for research. Good results require good data as part of a long-term solution. Rigor and data are the foundations of many successful technical public-private partnerships such as National Centers for Disease Control, the National Highway Transportation Traffic Safety Administration and the National Transportation Safety Board. Trusted public-private collaborations represent our mature adoption of technology and are an important step for cybersecurity to become a distinguishing capability for our Nation.

Understanding today's cyber threats to our communications networks is about more than war stories, anecdotes and scare tactics. Adversaries can combine supply chain and operational vulnerabilities in hardware, software, data and humans to create multitudes of attack strategies. Policies should address the root causes of our cyber threats and not just the immediate symptoms. Otherwise our adversaries will merely use another combination of what we haven't yet explicitly blocked, which is a continuously losing battle for cybersecurity.

For decades, the public sector, often in partnership with CERT, has addressed the technical symptoms and root causes of cybersecurity threats and attacks together. At CERT, we help millions of programmers write secure software to address the root cause of vulnerable software. We help agencies protect critical information, critical infrastructure operated by hundreds of private companies to address the challenges of responding to active attacks with potentially serious consequences. Using our decade-long work on resiliency management and smart grid maturity models, we are helping the Department of Energy, DHS and the White House with the Electricity Sector Cybersecurity Risk Management Maturity

Project. Such work will remove core vulnerabilities and decrease the impact of attacks.

To better understand cybersecurity problems and solutions, the science of cybersecurity is now broadly endorsed and funded by key Federal science and technology agencies including the Department of Energy. Policymakers can assist the research community by explicitly requesting cybersecurity innovations and practices that are scientifically and operationally valid. Furthermore, policymakers can request data owners, public or private, and the research organizations who can diligently use the data to provide appropriate access to high-fidelity operational data. Only with such data can cybersecurity researchers learn leading attack indicators, identify underlying principles and evaluate solutions.

Another role for the public sector is to improve the trust required for effective cyber attack preparation and response by clarifying public and private roles in cybersecurity, especially with respect to information sharing. Consider establishing one or more national repositories of operational cybersecurity data for research purposes. Access to such a repository would enable cyber research to reach new levels. Sharing cyber data with strong privacy controls would engender research that can look more globally and more predictably at the problem, especially in the long term.

In conclusion, every day we at CERT see the value of trust, rigor and data in helping mitigate cyber vulnerabilities, threats and attacks. We look forward to the day when our Nation can handle cybersecurity threats and attacks with the same efficiency and effectiveness as our Nation's response to the H1N1 health crisis. Then cybersecurity will truly be a distinguishing national capability alongside others such as our ability to innovate. Thank you.

[The prepared statement of Mr. Shannon follows:]

Testimony of Dr. Gregory E. Shannon
Chief Scientist for the CERT Program at
The Software Engineering Institute at Carnegie Mellon University
House Committee on Energy and Commerce
Subcommittee on Communications and Technology

"Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
March 28, 2012

Chairman Walden, Ranking Member Eshoo, and other distinguished members of the subcommittee, thank you for the opportunity to testify; it is my pleasure to discuss cybersecurity and the public sector response.

About the CERT® Program

The CERT Program is part of the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) sponsored by the Department of Defense and headquartered in Pittsburgh, Pennsylvania with facilities in Arlington, Virginia (www.sei.cmu.edu).

The CERT Program (www.cert.org) has evolved from the first computer emergency response team. CERT was created by the SEI in 1988, at the request of the Defense Advanced Research Projects Agency (DARPA), to respond to the Morris worm incident and related issues. The CERT Program continues to research, develop, and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, national, and international cyber incident responses. Over the past 23 years, CERT has led efforts to establish more than 200 computer security incident response teams (CSIRTs) around the world – including the Department of Homeland Security (DHS) US-CERT. We have a proven track record of success in transitioning research and technology to those who can implement it on a national scale.

I am Dr. Greg Shannon, the Chief Scientist for the CERT Program, where I lead efforts to sustain and broaden CERT's strategic research, development, and policy initiatives.

Testimony

The science of cybersecurity is still in its infancy; to prevail against the evolving cyber threats we need further research and innovation to better understand and inform us on the problem and the impact of solutions. As we have come to understand the threats, gain experience with pragmatic solutions, and consider the roles for the public and private sectors, we see two to opportunities for significantly improving cyber security. The first opportunity is to broadly promote the identification of and use of *scientifically and operationally validated* policies, best practices, technologies, standards, products, etc. The second is to actively enable the *controlled collection of and access to high-fidelity operational (real) data for research.* Such rigor and available data are the foundations of many successful technology-based public-private partnerships such as the National Centers for Disease Control (CDC), National Highway Traffic Safety Administration (NHTSA), or the National Transportation Safety Board (NTSB). These types of trusted collaborative environments are part of the natural maturation of efficient and effective technology transition and an important step in cybersecurity becoming a critical national capability.

The Threat

Understanding today's cyber threats to our communication networks is about more than just war stories, anecdotes, and scare tactics. Lawmakers need to understand the mechanisms that enable cybersecurity threats so that effective policies can be put in place to mitigate those threats. Everyone talks about malicious code, botnets, and phishing – which are all symptoms; to truly combat the problem you need to identify, understand and address the underlying vulnerabilities that enable the threats.

Policy should aim to treat the root causes of our cyber threats not just the immediate symptoms. Being overly focused to the symptoms of threat is not a long-term solution and can detract from real progress in fighting the threat. There are many kinds of cyber-attacks and they can be delivered in numerous ways. A cyber-attack relies upon multiple failures in the system to be successful – it is what makes combatting the problem so hard and total eradication likely impossible. However, when users and producers of software are armed with awareness of the techniques and approaches utilized by our adversaries they can begin to actively mitigate the problem.

Consider Figure 1 below that highly simplifies the elements and phases an adversary manipulates to create an attack, supported by a combination of failures. In a cyber ecosystem you have four main elements of vulnerably used to deliver a cyber-attack. They are hardware, software, data, and humans. Each of those elements has two exploitable conditions, a developmental and operational phase -these are the points of injection and/or realization of an attack. Vulnerabilities can be introduced unintentionally by human error or maliciously when an element is being built and/or being used. An adversary can "mix and match" the main approaches with points of insertion. So even in this generalized illustration, an adversary has over 600 combinations[1] of invasion strategies to choose from for a single instance of malicious effort. For example, Stuxnet utilized an inadvertent mistake made in the development of software to create both software and hardware failures during operation.

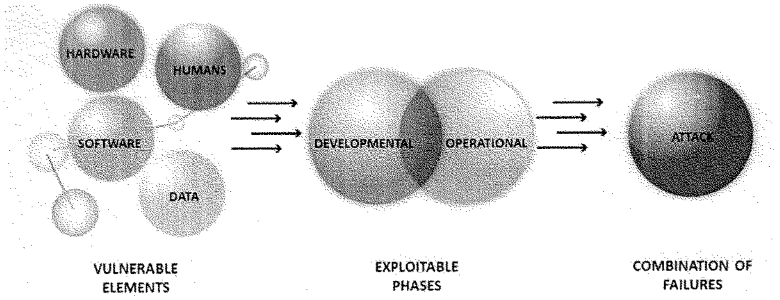


Figure 1: Formulating an attack – a combination of elements and phases.

[1] $(4!+1)^2 - 1 = 624$.

What the Public Sector Is Doing to Address Those Threats

For over two decades, the public sector, often in partnership with the CERT Program, has been addressing the technical symptoms and root causes of cybersecurity threats. Below, I highlight examples of three such activities. Secure coding initiatives seek to reduce well-understood coding errors in software. These errors are the foundation of malware and are exploited in most attacks. Critical Infrastructure Protection creates scalable capability for immediate response to serious threats and attacks, and resiliency efforts mitigate the symptoms of attacks while also amplifying the functionality and survivability of our communications infrastructure, in spite of vulnerabilities.

Secure Coding

Software vulnerabilities are a growing threat to governments, corporations, educational institutions, and individuals. Alongside private industry, many U.S. Government agencies including DoD, DHS, NSA, NSF, NIST, and others, are researching tools and techniques to remove coding errors so that systems can be developed free of software vulnerabilities.

As has been stated, by us and others, in previous hearings, many cyber vulnerabilities can be avoided with good cyber hygiene. The CERT Program has focused our research on international standards for secure coding in software, by taking a comprehensive approach to eliminating vulnerabilities and other software defects and utilizing detailed analysis of vulnerability reports originating from the U.S. Department of Defense (DoD) and other sources. As a consequence of analyzing thousands of vulnerability reports, CERT has observed that indeed most vulnerabilities stem from a relatively small number of well-understood types of programming errors. CERT has come to understand and share with software developers the practical steps to eliminate known code-related vulnerabilities by identifying the insecure coding practices and developing secure alternatives.

Using a wiki-based community process, CERT coordinates the development of secure coding standards alongside security researchers, language experts, and software developers. More than 500 contributors and reviewers have worked together in the development of secure coding standards on the CERT® Secure Coding Standards wiki.[2]

These new coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference. Moreover, they provide a metric for evaluating and contrasting software security, safety, reliability, and related properties; when applied during software development these coding standards can create more secure systems.

The Secure Coding team has made sizable contributions to the development of a major revision of the ISO/IEC standard for the C programming language,[3] which includes many security-informed changes.

[2] Seacord, Robert C. Secure Coding in C and C++. Upper Saddle River: Addison-Wesley, 2006, https://www.securecoding.cert.org

[3] http://www.sei.cmu.edu/newsitems/iso-standard.cfm

Critical Infrastructure Protection

The goal of a national critical infrastructure protection (CIP) program is to manage risks to critical infrastructures. In Presidential Decision Directive 63,[4] the White House described these infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private."

Since its inception, the CERT Program has supported critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP), both in the United States and abroad, with a mission to build competent cyber security management capabilities. The CERT Infrastructure Resilience Team has established a center of excellence focusing on information technology management that supports critical infrastructure and key resources (CI/KR).

We work with a diverse collection of CI/KR stakeholders, from owners and operators of the infrastructure itself to regulating bodies and the federal agencies with lead responsibility for sector performance and risk management. We produce tools, techniques, technologies, and training to raise awareness of the information security risks to CI/KR and to manage and improve resiliency.

Our research and outreach in CIP includes the following areas:

- Conducting research to identify new technologies and methodologies to be used by members of the CI/KR community to support protection efforts
- Conducting research to provide an understanding and perspective of CI/KR threats and vulnerabilities
- Capability development for national critical infrastructure protection programs
- Developing information security risk assessments and methodologies, guidelines, and best practices centered on CIP
- Collaborating with standards bodies to develop cyber security standards that support national CIP goals

Resiliency

The U.S. Government needs computing infrastructure that is not only more secure but also more resilient to mitigate the escalating threats. The need to focus on resiliency is gaining momentum – as understanding grows that we will not be able to thwart every attack and thus taking the needed measures to ensure the systems survive an attack, is crucial. Resilience depends on three key capabilities: resistance, recognition, and recovery. Resistance is the capability of a system to repel attacks. Recognition is the capability to detect attacks as they occur and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability, is the capability to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack.

Since 2001, the CERT Program has been working in the areas of security process improvement and operational resilience management and engineering. Through work that is focused on improving an organization's involvement in managing information security risks, we realized

[4] http://www.fas.org/irp/offdocs/pdd/pdd-63 htm

that organizations often view security as a technical specialty and don't usually associate it with other activities such as business continuity and IT operations management—all of which are focused on managing operational risk and sustaining operational resilience. Absent this important business driver, it is difficult to position security (or business continuity planning) as an enabler of an organization's strategy, much less an activity that is worthy of the investment of limited resources such as capital and people.

Through collaboration and extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, CERT codified a definition for operational resilience management processes called the CERT Resilience Management Model (RMM).[5] The model provides guidance for measuring the current competency of essential capabilities, setting improvement targets, and establishing plans and actions to close any identified gaps.

This work has been utilized in the current massive public-private effort under way to modernize the electric power grid to enable important advances in energy efficiency, reliability, and security. With the support of the US Department of Energy (DOE) and input from a broad array of stakeholders, the SEI has been tasked with the stewardship and advancement of the Smart Grid Maturity Model (SGMM[6]) since 2009.

More recently, working with the DOE and DHS on The Electricity Sector Cybersecurity Risk Management Maturity Project, a White House initiative this year, the SEI is a key participant in the creation of a model designed to help the electric sector evaluate their cybersecurity capabilities in a consistent manner, communicate capability levels in meaningful terms, and guide an organization in prioritizing cybersecurity investments.

What Role the Federal Government Should Play

While there are many roles for the Federal Government to improve cybersecurity, we discuss two today that, if well executed, could have bountiful near- and long-term benefits for the cybersecurity of our nation's communications networks. I'll explain both in further detail below, but in summary, they are:

> First, the Federal Government could explicitly encourage cybersecurity innovations and practices that are *scientifically and operationally valid.* This especially includes supporting access to data for experimental cybersecurity research.
>
> Second, the Federal Government can improve the trust required for effective cyber attack preparation and response by clarifying public and private roles in cybersecurity, especially with respect to information sharing.

Promote Scientifically Valid Innovation and Practices for Cybersecurity

CERT catalogues over 250,000 instances of candidate malware artifacts each month. At this volume it is difficult to determine in real time what is malicious, let alone what intent may be. To further muddy the waters, we still don't truly understand the properties and bounds of the

[5] Caralli, Richard A. , Allen, Julia H., and White, David W. CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience (SEI Series in Software Engineering). Upper Saddle River: Addison-Wesley, 2011

[6] http://www.sei.cmu.edu/smartgrid/

internet and its seemingly limitless dynamics. Consider the fallout of Michael Jackson's death: like never before people around the world flocked to the internet to follow the news, creating such a rush of internet traffic that, assuming it was under attack, Google returned an 'error message' for searches of the singer's name.[7] At least one of our uniformed military services had to restrict access to streaming video sites during Jackson's funeral to preserve sufficient bandwidth to ensure availability for operational and official administrative requirements.

The cyber community has now clearly recognized the current limits of our understanding. In response many federal science and technology agencies[8] have broadly endorsed and funded research into the science of cybersecurity.[9] For example, understanding intent, characterization, or presentation of properties and relationships from artifacts, is truly a hard problem, and is, in fact, the motivation behind DARPA's Cybergenome program.

Policymakers have the potential to play two important roles to enable progress in the science of cyber security. First, explicitly request that policies, best practices, technologies, standards, products, and large-scale operational plans are *scientifically and operationally validated.* Below are the definitions that we have provided to The House Homeland Security Committee:

> A result is *scientifically valid* when it is the product of a methodical process; when it is well documented, quantifiable, statistically sound, and reproducible; and when it produces principles that explain a testable class of phenomena. Results are analyzed for confounds; unmitigated confounds are identified and characterized.
>
> A result (report, technology, capability, practice, policy, or process) is *operationally valid* when it delivers in practice the measurable properties it was intended to deliver. Operational validity applies only to the properties actually observed, demonstrated, or measured in practice. For example, a capability realistically demonstrated on 1,000 systems is operationally valid for 1,000 systems, but not yet for 10,000 systems.

Second, work with both those who own the data and the research organizations, who can diligently use it, to provide appropriate access to high-fidelity operational data. Only with such data can researchers learn the leading indicators of cyber attacks. Such data also allows researchers to determine the baselines of typical cyber activity so that unusual events can be quickly and accurately interpreted as to their relevance and severity. Similarly, such data allows researchers to experiment with new approaches and technologies to quickly determine their potential efficacy in the real world.

Public and Private Roles to Promote Trust

I encourage the Members to reflect on the Center for Disease Control's (CDC) characteristics, as a trusted entity with technical excellence. The CDC's mission is to monitor health, detect and investigate health problems, conduct research to enhance prevention, develop and advocate sound health policies, implement prevention strategies, promote healthy behaviors, foster safe

[7] http://news.cnet.com/8301-17939_109-10274137-2.html

[8] NSF, DoD, DHS, DOE, NSA, NITRD, OSTP, and others.

[9] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

and healthful environments, provide leadership and training[10] and it seeks to accomplish this through partnerships and collaborations versus authorities.

Utilizing its role as a trusted partner, the CDC has unquestionably been able to execute successful national health responses. Consider the CDC's success with the H1N1 virus, in its own words:

> The global response to the 2009 H1N1 influenza pandemic that affected more than 214 countries and territories was the most rapid and effective response to an influenza pandemic in history. Investigations of the virus' origin, severity, and spread revealed those potentially at risk, and surveillance data were used to estimate the rate of illness and guide the response in real time. Within two weeks of detecting the virus, diagnostic tools were provided to laboratories in 146 countries resulting in more than an 8-fold increase in specimen submissions. Collaborative laboratory and clinical training was provided to more than 6,100 health professionals in 34 countries. Through an international donation program, the vaccine was made available to 86 countries.[11]

Imagine a similar approach dedicated to the cyber health of the nation – and the potential to tell the same story about the next Conficker or Stuxnet. With a clear point of interaction to provide the origin, severity, spread, surveillance, analytical tools and inoculation of and,against cyber threats, endorsed by and coordinating with the federal government, organizations would have an unbiased trusted agent serving as a national cyber-security aggregation and coordination center.

Another important CDC-related property is the ability to maintain a national repository of cyber threat information for research purposes. There are several organizations that have malware repositories, but the repositories are seen as a competitive advantage and are rarely shared. Access to such a repository would enable cyber research to reach new levels. Currently researchers work with only small pieces of the puzzle, most often the symptoms, resulting in reactive research. Sharing cyber data, like public health data, with a strong emphasis on privacy, would engender research that can look more globally and more predictably at the problem. Furthermore, it would allow cyber epidemiology to reach new levels of quality. Epidemiology, a cornerstone of public health research, identifies distribution and determinants of health-related states or events[12] which in turn can guide policy decisions and evidence-based medicine. Armed with a well-maintained repository, with appropriate controls on access (it is important to recognize that the CDC has in fact been able to accomplish first-class research and achieve information sharing while successfully dealing with privacy issues), a trusted cyber collaboration could provide more effective methods for basic cyber hygiene.

A clear point of interaction for government agencies, as well as other public and private entities, could shape decisions for the greater good based on the highest quality data, openly acquired and objectively analyzed. However structured, this organization would be charged with working with partners throughout the nation and the world to collaboratively create the expertise, information, and tools that people and communities need to protect themselves.

[10] http://www.cdc.gov/about/organization/mission.htm

[11] A National Strategic Plan for Public Health Preparedness and Response – September 2011, http://www.cdc.gov/phpr/publications/2011/A_Natl_Strategic_Plan_for_Preparedness_20110901A.pdf

[12] http://www.who.int/topics/epidemiology/en/

Conclusion

In spite of the complexity and scope of the threats to our nation's communications infrastructure, the real long-term opportunity for improving cybersecurity it to promote *scientific and operational validity* for policies, best practices, technologies, standards, products, etc., and to actively enable the *controlled collection of and access to high-fidelity operational (real) data for research.*

Every day, we in the CERT Program see the value of such rigor and data, such as our work on secure coding, resiliency, and critical infrastructure protection. We look forward to the day when the nation can handle cybersecurity threats and attacks with the same efficiency and effectiveness as our nation's response to the H1N1 health crisis. I believe that with data and through science we can make efficient and effective cybersecurity a critical national capability enjoyed by all.

Mr. WALDEN. Doctor, thank you. We appreciate your testimony.

And our final witness on the panel is Roberta Stempfley, Acting Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security. We are delighted to have you here this morning and we look forward to your testimony.

STATEMENT OF ROBERTA STEMPFLEY

Ms. STEMPFLEY. Thank you very much, Chairman Walden and Ranking Member Eshoo. As you said, I am with the Department of Homeland Security. I have two decades of experience as a public servant working both in the Defense Department for 18 years and now almost two years at the Department of Homeland Security, and it is certainly a privilege for me to have the opportunity to come and speak to you today about the efforts that the Department of Homeland Security has that support the cybersecurity of our important communications networks.

As you know, the private sector owns most of the national infrastructure in the communications environment and as such, protecting the communications networks is not something the Federal Government can or should do alone. There is no silver bullet to cybersecurity, as my esteemed panel colleagues have indicated. There is not a single tool, a single technique nor a single organization who is capable or accountable or responsible for delivering cybersecurity to the communications networks. But access to reliable and consistent communications is essential to maintaining the Nation's health, safety, economy and public confidence.

Protection of communications infrastructure from this range of threats, national disasters, terrorism and cybersecurity, is of the highest priority to the Department of Homeland Security, and this communications infrastructure is complex. It is a system of systems with multiple ownerships and multiple interconnection points. It involves wireline, wireless, satellite, broadcast capabilities and serve the transport and enable this Internet that we live, play and function on.

The Office of Cybersecurity and Communications in the Department's National Protection and Programs Directorate is designated the federal entity to lead the coordination with both the communications and information technology sectors of critical infrastructure. We work closely with these partners and ensure robust and resilient communications throughout the Nation.

Within this Office of Cybersecurity and Communications, we have an organization called the National Communications System, which is the lead for the communications sector. It leads government-industry coordination critical in the planning, initiation, restoration and reconstitution of national security emergency preparedness service and facilities. The National Cybersecurity Division is responsible for leadership in the information technology sector and responsible for major cybersecurity programs that we will be speaking of today.

Additionally, we have the Office of Emergency Communication, which supports and promotes the ability in emergency responders and government officials to communicate in the event of a disaster. The Office of Emergency Communication's focus is on that interoperable and operable emergency communications nationwide.

All of these organizations and others come together in an operation center called the National Cybersecurity Communication and Integration Center. It houses the National Coordinating Center for Communications, a part of the National Communications System, the U.S. Computer Emergency Readiness Team, a part of the National Cybersecurity Division, as well as other partners from industry and across the Federal Government including members of the Communications, Information Sharing and Analysis Center. Our collective efforts tie into the DHS-wide collaboration and extend our partnership with Federal, State, local governments and the private sector, and together we work under orchestration to negate threats to the communications infrastructure and to build strategies for future success.

Protection of that communications infrastructure is conducted in this holistic fashion and encompasses physical and cyber threat strategies. Partnerships are key and very important as is two-way information sharing. We have this information sharing real time on the floor, as I indicated, where 5,200 alerts were released by U.S. CERT to our partners over the course of the last year. The Department employs mechanisms to ensure that the sensitive propriety information shared with us from industry is protected and that privacy and civil liberties are upheld. It is industry's willingness to share this information on a voluntary basis that speaks to the strong trust between DHS and its private-sector partners as we work forward in this situation.

I spoke to that Communications Information Sharing and Analysis Center. There are information sharing and analysis centers within each sector. They are sector specific. And in that sector, we have 56 private-sector partners that were the first operations entity from the private sector on the floor of the National Cybersecurity Communications Integration Center.

In addition, in the Department, the Secretary serves as the executive agent supporting the President's National Security Technology Advisory Committee. This committee is comprised of up to 30 chief executives from industries like network service providers, telecommunications, information technology, finance and aerospace companies. The NSTAC makes recommendations to the President on strategies and practices to secure vital communications links through events and crises. We also have worked in partnership on communication sector supply chain threats, an item of interest to the committee today.

Given the increasing use of technologies such as smartphones by first responders, there are real innovations available in that situation and the Public Safety Broadband Network that this committee was so integral in establishing must be secure and reliable so that emergency responders can be assured that sensitive information is protected and accurate. DHS is committed to working with all of our public- and private-sector partners today including NTIA and the FCC, who I am pleased to be with on the panel today, to ensure we secure the National Public Safety Broadband Network through this holistic approach with equal emphasis on protecting confidentiality, integrity and availability.

Thank you again for this opportunity to testify, and I am pleased to answer your questions.

[The prepared statement of Ms. Stempfley follows:]

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

Testimony of Roberta Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Energy and Commerce Committee
Subcommittee on Communications and Technology
Washington, DC

March 28, 2012

Hearing on
Cybersecurity of Communications Networks

Chairman Walden, Ranking Member Eshoo, and distinguished members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) efforts to secure communications networks. Before I begin, I would like to thank the Committee members for their leadership and dedication to supporting enactment of legislation to create a Nationwide Public Safety Broadband Network. As you know, this was one of the 9/11 Commission recommendations and one of the Administration's priorities over the last year. We look forward to continuing to work with the Committee to implement these efforts and build a nationwide, interoperable network for emergency responders.

In addition to our emergency communications work with public safety agencies, the Department works closely with the communications industry to ensure a resilient, reliable, and available communications infrastructure. Today I will provide an overview of the communications infrastructure, the Department's mission as it relates to the protection of the communications infrastructure, and the coordination of this mission with our public- and private-sector partners.

As communications technology evolves, the Federal Government must also evolve. The Government must make advances alongside industry to ensure that the Government has access to tools that allow it to communicate internally and with the public in all circumstances. It is also critical that as communications technology evolves, this advancement includes appropriate security. Accomplishing this goal requires the Federal Government to develop strategies to address challenges inherent in emerging, and often game-changing, technologies. Public safety agencies are increasingly relying on these emerging technologies. Further, the Nation's newfound reliance on mobile devices and applications, as well as on social networking tools, to communicate presents both opportunities and challenges. Because the private sector owns much of the Nation's infrastructure, protecting it is a responsibility that the Federal Government cannot, and should not, shoulder alone. Instead, we must collaborate closely with our public- and private-sector partners.

The Communications Infrastructure

Access to a reliable and resilient communications network is essential to maintaining the Nation's health, safety, economy, and public confidence. As such, protection of the communications infrastructure from threats of natural disasters, cyber attacks, and terrorism is among the Department's highest priorities. The Department has committed resources to addressing this.

The Nation's communications network is a complex system of systems, which incorporates multiple technologies and services with diverse ownership. This infrastructure includes wireline, wireless, satellite, cable, broadcasting capabilities, and the transport networks that support the Internet and other key information systems the Government depends upon every day. The communications companies that own, operate, and supply the Nation's communications infrastructure have historically factored natural disasters and intentional and accidental disruptions into network resilience architecture, business continuity plans, and disaster recovery strategies. As the industry transitions from point-to-point (circuit switch) to router-to-router (packet switch) technologies, DHS continues working with private-sector companies to implement strategies critical to protecting the infrastructure.

The interconnected and interdependent nature of these service-provider networks has for decades fostered crucial information sharing and cooperative response-and-recovery relationships. Even in today's highly competitive business environment, the community has a long-standing tradition of cooperation and trust, which is imperative because problems with one service provider's network inevitably impact the other providers.

Providing coordinated and collaborative protection of these networks requires the Department to foster and maintain strong public-private partnerships, which improve planning, information sharing, and support response and restoration of the infrastructure when disruptions occur. While it is impossible to eliminate all vulnerabilities to communications infrastructure, the Department works with the private sector to make strategic improvements in security that minimize the likelihood of disruptions.

The Department's Communications Infrastructure Protection Mission

The Department's role in the communications infrastructure, as outlined in the Homeland Security Act of 2002, Homeland Security Presidential Directive (HSPD) 7, and Executive Order 12472, is to engage with Federal, state, local, tribal and private-sector partners to lead national-level efforts to enhance the overall protection of the communications infrastructure. As we have learned while protecting the Federal civilian government networks, cyber threats are unpredictable and evolving. Malicious actors continue to target the Nation's critical infrastructure, affecting our national and economic security.

We must continue designing a collaborative strategy that keeps our networks available, resilient, and reliable.

As the Sector Specific Agency under HSPD-7 for both the communications and information technology (IT) sectors, DHS, through the National Protection and Programs Directorate (NPPD)'s Office of Cybersecurity and Communications (CS&C), works closely with the communications and IT sector to ensure robust and resilient communications throughout the Nation. Within NPPD/CS&C, the National Communications System (NCS) leads this activity for the communications sector and the National Cyber Security Division (NCSD) works with the information technology sector. The National Cybersecurity and Communications Integration Center (NCCIC) houses the National Coordinating Center for Telecommunications (NCC), NCS's operational arm. The NCS leads the government-industry coordination critical in the planning, initiation, restoration, and reconstitution of national security/emergency preparedness (NS/EP) services and facilities. NPPD/CS&C's Office of Emergency Communications (OEC) supports and promotes the ability of emergency responders and government officials to continue to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters. OEC works to ensure, accelerate, and attain interoperable and operable emergency communications nationwide. NPPD's collective efforts figure into a DHS-wide collaboration that extends to our partnerships with relevant Federal agencies, state and local governments, and the private sector. Together, these organizations are working to develop strategies to protect and mitigate threats to the communications infrastructure.

The security of the communications sector relies significantly on the IT sector. In recognition of this reliance, NCS and NCSD, as the Communications and IT Government Coordinating Council (GCC) chairs respectively, together with the relevant Sector Coordinating Councils (SCC), work closely on the policy and operational issues affecting both sectors. Each fall, the Communications and IT GCCs and SCCs hold the annual IT-Communications Sector Quad meeting, which brings together the government and private-sector stakeholders to discuss efforts and activities underway in each sector. Discussions cover efforts undertaken both independently and in partnership with each other and address issues affecting both sectors, including the cybersecurity of the two sectors.

Specific Programmatic Activities

The National Communications System

The NCS is an interagency system comprised of the telecommunications assets of 24 Federal agencies, each with significant operational, policy-related, regulatory, and enforcement responsibilities. The NCS coordinates telecommunications preparedness, response, and restoration activities across its 24 member agencies through the NCS Committee of Principals, which consists of senior government officials from each of the 24 member agencies, ensuring a diverse representation that includes the full range of Federal telecommunications assets. The NCS also coordinates responses with stakeholders through the National Security Telecommunications Advisory Committee (NSTAC) and the NCC.

While cyber threats often necessitate unique assessment and mitigation strategies, protection of the communications infrastructure is also conducted in a holistic fashion, encompassing both physical and cyber threat mitigation strategies. Therefore, the Department leads national-level initiatives that are critical to addressing communications challenges associated with cyber attacks, deregulation, natural disasters, and terrorist attacks on our Nation. These efforts include risk assessment and management, technology enhancement, response coordination, and improvement of public-private bidirectional information sharing.

The NCS leads a number of risk assessment and management efforts, which improve the overall security of the communications infrastructure. For example, the NCS, through its partnership with the private sector, works to identify and mitigate vulnerabilities of those critical infrastructure interdependencies and dependencies. These partnerships facilitate the sharing of proprietary information in a secure environment on shared vulnerabilities in the communications sector, resulting in the ability to model and simulate wide-spread disruptions to the infrastructure. The Department employs mechanisms to ensure that sensitive and proprietary information is protected. The industry's willingness to share this information on a voluntary basis speaks to the strong trust between DHS and its private sector partners and the recognition that protection of our infrastructure is shared. Ultimately, these risk assessment and management efforts enable the sectors to incorporate, through coordination and collaboration, stringent security standards into those NS/EP technologies.

Under the National Infrastructure Protection Plan (NIPP), the NCS and the private sector jointly produce the Communications Sector Specific Plan (CSSP). The CSSP incorporates timely solutions and details a risk-management process that identifies and protects nationally critical architecture, ensures overall network reliability, maintains "always-on" services for critical customers, and quickly restores critical communications functions and services following a disruption. The development and implementation of the CSSP encourages public and private-sector partners to enhance the Nation's communications infrastructure protection framework. Sector partners will need to prioritize the actions set forth within this plan and coordinate their implementation accordingly.

NCS is working with its government and industry partners to mitigate cybersecurity threats to the communications infrastructure. For example, CSSP identifies specific risk management programs that mitigate cybersecurity threats, including the 2012 National Sector Risk Assessment (NSRA) and Supply Chain Working Group. In addition, NCS participated in cybersecurity testing and response capabilities during National Level Exercise 2011 Eagle Horizon and Cyber Storms II and III Exercises. NCS also led a cyber working group that evaluated how vulnerabilities impact the confidentiality and integrity of a network's data, as well as the availability of a network to meet the needs of its users. The working group focused on six broad categories of cyber risk across broadcasting, cable, satellite, wireless and wireline networks. The 2012 NSRA will address cyber risks, as well as physical and human vulnerabilities, which may include supply-chain risk to the communications infrastructure.

National Security and Emergency Preparedness Communications

Incorporating security at the beginning of technology development or enhancement remains a priority for DHS with regard to NS/EP communications and cyber challenges. NCS is engaging in a number of initiatives to ensure security requirements are addressed throughout the acquisition lifecycle of all products and services. For example, through the development of its Next Generation Networks Priority Service Program, the NCS is working with the private sector to conduct in-depth cybersecurity analyses that identify security risks on the infrastructure that threaten NS/EP communications. A critical component of ensuring proper security is modeling and analysis. The NCS leads modeling, analysis, and technology assessments of current and future protocols, algorithms, network designs, and capabilities that will impact priority service communications in legacy and next-generation networks.

Playing a role in standards setting is also critical to ensuring that cybersecurity features are incorporated into the communications infrastructure. NCS participates in domestic and international standards-forming and -setting bodies to ensure that security considerations are appropriately addressed, including the International Telecommunications Union , the Internet Engineering Task Force and the Institute of Electronics and Electrical Engineers. These efforts lead to the development and implementation of national and international standards and ensure adoption of non-proprietary solutions for the United States' NS/EP communications industry-wide. International adoption of standards directly advances the United States' national and economic security interest by reducing the threats to our infrastructure and enabling our leadership and first responders to communicate during times of crisis.

Public-Private Partnerships

NCS has become a recognized means for the secure sharing of proprietary information among government and private-sector partners. For example, NCS formed the Network Security Information Exchanges (NSIE), a forum where government and industry share sensitive (proprietary) information. This information includes threats to operations, administration, maintenance, and provisioning of systems supporting the communications infrastructure in a trusted environment. The Federal Government membership has historically included representatives from the Intelligence Community and the Departments of Justice, Homeland Security, Defense, and Energy. As an all-voluntary forum, the group meets to identify intrusion activities, vulnerabilities that may lead to intrusion and exceed permission, significant malicious code, hackers, and other threats to the public network. This information is shared in real-time across government and private-sector partners through the US-CERT web portal.

Communications Information Sharing and Analysis Center

Information Sharing and Analysis Centers (ISACs) are an effective private-sector information-sharing and analysis mechanism. ISACs are sector-specific entities that advance physical and cyber critical infrastructure protection efforts by establishing and maintaining frameworks for operational interaction among members and external sector partners. The Communications ISAC (COMM-ISAC) leverages the interagency and public-private capabilities of the NCC and supports the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency. As a consortium of over 56 private-sector partners, the COMM-ISAC provides the NCC with situational and operational information on a regular basis, as well as during a crisis, and provides information to NCS. NCS, in turn, shares information with the White House and other DHS components. This information exchange is vital for ensuring the protective posture of both the communications and IT sectors.

National Coordinating Center for Telecommunications

The NCC is the 24x7 operational arm of NCS and works closely with other coordinating bodies across Federal, state, and local governments, as well as the private sector. The NCC assists in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities. The NCC serves as the center for voluntary collaboration; information sharing; and vulnerability, threat and anomalies assessments to the communications infrastructure.

The President's National Security Technology Advisory Committee (NSTAC)

The Secretary of DHS serves as the Executive Agent for the NCS, which provides support to the President's NSTAC. The NSTAC is composed of up to 30 chief executives from industries like network service providers and telecommunications, information technology, finance, and aerospace companies. The NSTAC makes recommendations to the President on strategies and practices to secure vital telecommunications links through any event or crisis, as well as help the Government to maintain a reliable, secure, and resilient national communications infrastructure. Fulfillment of these responsibilities often take place across five key themes: strengthening national security, enhancing cybersecurity, maintaining the global communications infrastructure, assuring communications for disaster response, and addressing critical infrastructure interdependencies and dependencies.

National Cyber Security Division

NCSD is charged with securing the Nation's critical information infrastructure. To achieve its mission, NCSD works with public, private, and international partners to secure cyberspace and the Nation's cyber assets.

Communications Sector Supply Chain Threats

NCSD has partnered with both NCS and the communications sector to address Information and Communication Technology (ICT) supply-chain threats, which increasingly pose a risk to the ability of the Federal Government and critical infrastructure to engage in mission-essential functions. Due to the amount of communications infrastructure critical for public sector functions that is owned and operated by the private sector, the Supply Chain Risk Management (SCRM) program within NCSD, in coordination with NCS, is developing a partnership between government and industry to adequately address these supply-chain concerns and collaboratively share relevant threat, vulnerability, and impact information with the CSCC. An interagency working group was formed to identify SCRM best practices, mitigation opportunities, and long-term planning to institutionalize effective models for SCRM across the sector. The group identified gaps in the Federal Government's understanding of telecommunications infrastructure, in both the Government's and private sector's understanding of the threat, and in the Government's access to an appropriate risk model to manage the supply chain. Through this evolving partnership, the NCSD is working to better identify and mitigate supply-chain security risks associated with sensitive elements of the telecommunications infrastructure.

The Information Technology Sector Specific Agency (IT SSA)
NCSD, as the IT-SSA, is the lead Government representative for the public-private partnership to secure national IT infrastructure. NCSD works with public and private sector partners to implement the IT Sector Specific Plan and risk management framework to assure the security and resiliency of the IT Sector. Additionally, NCSD facilitates cybersecurity sector-wide and cross-sector risk management across the U.S. critical infrastructure sectors through formal engagement; development of sector cybersecurity strategies; cyber infrastructure identification methodologies; and alignment of cybersecurity risk management approach with sector security strategy, risk assessment, and protective measures initiatives.

NCSD also leverages the sector partnership framework to work on cybersecurity issues that stretch across critical infrastructure sectors, including the communications sector, specifically through the Cross Sector Cyber Security Working Group (CSCSWG). The CSCSWG is a body with members drawn from each of the 18 critical infrastructure sectors, ensuring cross-sector collaboration on the cybersecurity issues facing all sectors.

Office of Emergency Communications

Nationwide Public Safety Broadband Network
Following the tragic events of September 11, 2001, members of the emergency response community – police officers, firefighters, emergency medical service (EMS) personnel – have worked with DHS to strengthen their emergency communications capabilities through enhanced coordination, planning, training, and new equipment. The creation of OEC was an important step toward improving the communications capabilities of those who are often the first to arrive at the scene of an incident—the Nation's emergency responders.

Recent developments in high-speed, wireless communications technology have presented an opportunity to provide public safety members with enhanced capabilities to share information and communicate during emergencies and day-to-day operations. Through the President's Wireless Innovation and Infrastructure Initiative (WIII), the Administration outlined its commitment to the development and deployment of the Nationwide Public Safety Broadband Network (NPSBN) for use by emergency responders in all parts of the country. This initiative supports a key recommendation from the National Commission on Terrorist Attacks Upon the United States, which called for the establishment of a nationwide, interoperable public safety communications network to resolve the communications challenges faced by emergency responders seeking to rescue victims and restore order.

The prospects of having a nationwide interoperable broadband network took a major step forward when the "Middle Class Tax Relief and Job Creation Act of 2012," was signed into law on February 22, 2012. Title VI of the new law, "Public Safety Communications and Electromagnetic Spectrum Auctions," advances key components of the President's WIII, including provisions to fund and govern the NPSBN. One of the most critical aspects of the law is the creation of a nationwide governance structure to oversee the network. The Administration believes that oversight is critical to ensuring that the NPSBN is a secure network that provides fully interoperable capabilities for all of our Nation's first responders.

To ensure oversight and governance of the network, the new law establishes the First Responder Network Authority (FirstNet) within the Commerce Department's National Telecommunications Information Administration (NTIA). Among its many responsibilities, FirstNet is directed to take "all actions" needed to ensure the construction, development, and deployment of the NSPBN, in consultation with Federal, state, local, and tribal public-safety entities. FirstNet is also required to ensure the safety and resiliency of the NPSBN, including protecting and monitoring against cyber attacks. As one of three Federal representatives on the FirstNet board, the Secretary of DHS will work with her Federal counterparts and the appointed members of the Board to ensure the successful deployment, governance, and operations of the NSPBN.

The deployment and security of this nationwide network will require significant collaboration among officials at all levels of government and the private sector, particularly with respect to leveraging existing partnerships and forging new ones to ensure the network is interoperable, secure, and state-of-the-art.

OEC is supporting the deployment of this network by continuing to work closely with the Departments of Commerce and Justice, as well as the Federal Communications Commission, on early implementation and planning efforts. In addition, OEC continues to work directly with Federal, state, local, and tribal stakeholders to provide policy guidance and planning assistance related to broadband emergency communications. Further, OEC has been tasked with continuing to coordinate with key DHS components and state and local public safety entities to ensure implementation of the envisioned nationwide network.

Under the strategy and policy direction of the One DHS Emergency Communications Committee, DHS has initiated a joint program management office to capture and implement Department-wide broadband requirements to develop a next generation tactical communications mobile platform for voice, data and video. This approach will align with commercial broadband technologies and public safety roadmaps to ensure cost efficiency and interoperability with Federal, state, local, and tribal partners.

These Federal coordination activities will be especially important in leveraging Federal expertise and assets in the areas of infrastructure protection and cybersecurity. Also, through its relationships with long-standing state and local collaboration groups, such as the SAFECOM Executive Committee/Emergency Response Council and the National Council of Statewide Interoperability Coordinators, OEC will continue to engage key public-safety leaders on a variety of issues regarding the development of the NPSBN, including security risks.

Securing the NPSBN

Once the NPSBN is deployed and operating, the network will increase communications interoperability, coordination, and response effectiveness by providing emergency responders with cutting-edge technologies and capabilities. However, we cannot overlook the security challenges that a new Internet Protocol (IP)-based communications network may also present. The NPSBN will interconnect many systems previously independent via IP networking, including public safety IT systems that transmit sensitive data, such as law-enforcement information and electronic medical records. While access to this data can help responders do their job more efficiently and effectively, it also presents new security risks, as this data could be highly valuable to cyber criminals and hackers.

That network must be secure and reliable so emergency responders can be assured that sensitive information is protected and accurate. Without careful planning on the front end, the NPSBN may find itself vulnerable to cyber attacks. As such, DHS has begun to examine potential security issues to the NPSBN and is well-positioned to assist FirstNet in building security into the foundation of the network. OEC, for example, is working with several stakeholder groups, including the National Public Safety Telecommunications Council and their established working groups, to discuss security issues for the NPSBN and to develop requirements. We will also leverage NCSD's work in the areas of standards and best practices from the cybersecurity community.

Together, OEC, NCSD, and NCS have started a risk assessment of the NPSBN. Since the Middle Class Tax Relief and Job Creation Act of 2012 was enacted, OEC has offered NTIA this continued assistance. OEC will coordinate with the necessary partners to conduct the assessment and will leverage NCSD's proven experience in cyber risk assessment methodologies. NCS will also provide input to the process based on past experience with risk assessments for the Communications Sector. The risk assessment will evaluate levels of risk in NPSBN physical infrastructure, data stored or transmitted on the network, and operational control systems. It will also help define, quantify, and prioritize risks. OEC will leverage the work done in this area by other partners, including the National Institute of Standards and Technology Public Safety Research Center. The risk assessment is expected to establish a process for managing cyber risks to the NPSBN, based on real-world experience and knowledge, which can be repeated as needed during the development and deployment of the NPSBN. DHS expects this to be the first of many ways in which the Department can work with and on behalf of FirstNet.

Securing the NPSBN requires a holistic approach, with equal emphasis on protecting confidentiality, integrity, and availability. It also requires a collective effort from public safety, network managers, and industry partners to ensure that cybersecurity is built into the NPSBN from the bottom up. The work that public safety agencies, Federal partners, and industry are doing to ensure effective and secure network operations is a significant start, and DHS looks forward to continued partnerships with government and private-sector stakeholders to build a secure communications network for our Nation's first responders.

Thank you again for this opportunity to testify. I am pleased to answer your questions.

Mr. WALDEN. Thank you, Ms. Stempfley. We appreciate your comments. We were just talking here about, as you described, the center out here, about maybe the subcommittee coming out to take a look at some point.

Ms. STEMPFLEY. We welcome you. Any time you would like, we would more than honored to have you out there and show you the span of activity that goes on in that center. As I said in my comments, it is a place where government and industry come together. We have representative not just from the communications sector but from the information technology sector, from the financial sector and from other partners on that floor as well as partners across government from the intelligence community and others.

Mr. WALDEN. All right. Thank you.

My first question would be to you. The Department of Commerce's Economic Development Administration recently suffered a cyber attack that has left the agency without network connectivity for several weeks, I am told. Could you elaborate on that situation and what DHS has been doing to address it, and has it been resolved?

Ms. STEMPFLEY. The Department of Homeland Security has responsibility for protection and defense of the Federal executive civilian branch including the Department of Commerce includes responsibilities for supporting the Department when they had a compromise of the nature that you are describing at the EDA. We have individuals on the ground with Commerce to support EDA in the reconstitution of their network and are building it in a way that is supportive of increased security and the meeting of the Federal standards that are initiated both by the Department and the Federal Information Security Management Act.

Mr. WALDEN. So are they still offline?

Ms. STEMPFLEY. I am personally not sure, sir, at the moment but we would be happy to follow up with you on that.

Mr. WALDEN. Any idea where the attack came from?

Ms. STEMPFLEY. I don't know attribution in this situation. Attribution is generally the responsibility of law enforcement and the intelligence community. We are responsible for protection and mitigation measures, and I am happy to come back with our partners from Commerce.

Mr. WALDEN. That seems pretty major if it has been offline for several weeks.

There has been a resounding call for increased consumer education when it comes to cybersecurity, and this is kind of for everybody here. However, a report released earlier this month by Trust Wave showed that after studying more than 300 data breaches in 2011, nearly 5 percent of the passwords on the compromised networks were variations of the word "password." So if end users cannot even wrap our heads around not using the word "password" as a password, how can we as policymakers form a better understanding of a complex topic like route hijacking? Does anybody want to take that one quickly?

Mr. SHANNON. At Carnegie Mellon University, there is a large number of researchers studying how to make security and privacy usable and it is turning out to be very daunting. The password research has shown that people do reuse passwords. When you get populations of passwords together, it creates a vulnerability. So it becomes clear that individuals—it is difficult for us to rely on individuals to be the foundation of security.

Mr. WALDEN. I want to ask a different question of you, Dr. Shannon. Some of the vulnerabilities in compromised systems persist despite common knowledge among computer programmers of the problem. For example, "SEQUEL," the Structured Query Language injection, has been one of the most common vectors for database attacks for years, I am told. How do we change the culture at coding to ensure the security is more of a focus?

Mr. SHANNON. One is by providing explicit guidelines, which we have been doing for the last 10 years. "SEQUEL" is not a language that we have tackled. We have been focused on C++ and Java and the C programming language. Part of the challenge is that we do not control where the programs are written so they may be written offshore under economically stressed and time constraints. So it is a challenge of improving the general practice and by providing coding standards is our step in that direction.

Mr. WALDEN. All right. Thank you.

Mr. Hutchinson, you recommended, I think, four points of things we should look at and talked about the supply chain issues and this notion of precompromises of hardware with malware installed. Are there more examples of that we should be aware of in this setting?

Mr. HUTCHINSON. In this setting, I can't cover. The examples I am aware of are classified. But, you know, I would very much welcome a classified discussion on that topic.

Mr. WALDEN. Could you speak more about the malicious data modification issues in this setting? What does that mean? What are we seeing as examples?

Mr. HUTCHINSON. So just for context, when you—when an event occurs on a network, the most normal thing for an analyst to do is to look for the exfiltration of data from that network, to analyze malicious code to determine whether it is stealing data from the network and pointing it in the direction of the adversary. The malicious modification would be something that the compromise leaves behind that alters the data, changes the nature of the data, changes emails, things like that.

Mr. WALDEN. I see. OK. And a question I have asked all the panels we have had before, sort of in with the Hippocratic oath, first, do no harm. Do you each, could you real quickly just say what is the one caution you could offer as we promulgate legislation? Ms. Alexander, what shouldn't we do?

Ms. ALEXANDER. I think it is important that as you consider ways to deal with this important issue, there is a grounding and understanding of how the network actually works so that the rules that are developed don't inadvertently undercut some of the other activities.

Mr. WALDEN. All right. Admiral Barnett?

Mr. BARNETT. So I think it is important to make sure that we don't cut off this engine of innovation, that as we move forward that we continue to have that openness. But I would also say that as you do it, you have to look at the performance metrics. Are the things that we are doing actually having some effect? We have to have data driven to make sure that we are actually doing some good.

Mr. WALDEN. Mr. Hutchinson?

Mr. HUTCHINSON. So there are some very strong relationships in helping this problem like the relationship between DHS and NSA. Anything that would harm that relationship I think would be hurtful to the government.

Mr. WALDEN. Keeping open communication?

Mr. HUTCHINSON. Yes, that communication and the relationship between the NSA and applying classified approaches to this otherwise unclassified problem I think is extraordinarily valuable.

Mr. WALDEN. OK. Dr. Shannon?

Mr. SHANNON. I think we need to protect innovation, as the admiral mentioned. There is a balance between too little security that allows for the loss of intellectual property and then onerous security that imposes a tax on innovation in the long term and makes us no better than other countries that are more restrictive in how their citizens behave, so I think there is a real balance to maintain there to promote innovation.

Mr. WALDEN. All right. Ms. Stempfley?

Ms. STEMPFLEY. As several individuals have identified, there are relationships and partnerships and multiple organizations that are involved, and those relationships must equally be sustained and we must continue to empower the multiple organizations that are involved here.

Mr. WALDEN. Thank you all very much.

Now I turn to Ms. Eshoo for questions.

Ms. ESHOO. Thank you, Mr. Chairman, and to each of the witnesses, thank you. Excellent testimony. There was a group of students that were here, and you are facing this way, but I couldn't help but notice that they all left en masse, and I thought we have either scared the hell out of them or bored them. I don't know. I think that that might apply to us as well because there are so many moving parts to this.

I have a whole list of very specific questions but I want to set those aside. I will put them in writing to you, and I don't think we need to ask for unanimous consent, no, because members can ask questions in writing of the witnesses.

When we look at the whole issue of cybersecurity, it is my understanding that 5 percent responsibility in the public sector, the government. Ninety-five percent of this rests with the private sector. Now, CSRIC has come up with some recommendations. Both the chairman and myself and I think that other members have referenced it. Maybe some of you did in your testimony. But I want to ask you the following question, and I appreciate the rather deep dives that you have done on your specific area of expertise and what your observations are. But for each one of you, on the 5 percent, which is the government, what is the top recommendation that you would make to us that we need to take into consideration that will help remake the landscape into a very smart one to address the threats that come to us relative to cybersecurity in the government. Ms. Alexander, I don't have a lot of time. We have got, like, 3 minutes for five of you.

Ms. ALEXANDER. Sure. I think in addition to this idea of continuing innovation and voluntary codes of conduct, government is very powerful as a user and so we can set examples and we influence procurement patterns. I think that is one of the most powerful things that we can do as government.

Mr. ESHOO. Excellent. Thank you very much.

Admiral, thank you for your wonderful work.

Admiral BARNETT. Thank you, ma'am. So I think continuing to seek voluntary and industry-based solutions is the bedrock, incentivizing that and looking for that, and then obviously as almost every person mentioned in your openings, we really have to tackle the supply chain.

Ms. ESHOO. Thank you.

Mr. HUTCHINSON. So maintaining opt-in alternatives for industry to seek government's help in incentivizing those I think is critical, and the supply chain is an area that will become increasingly problematic, and I think we need to work hard with industry to take the government know-how.

Mr. SHANNON. I would say trust is——

Ms. ESHOO. Excuse me. I am sorry, Dr. Shannon. Let me get back to you, Mr. Hutchinson. Are you suggesting that practices on the public side is something that the private side can gain a great deal from, or is it the other way around?

Mr. HUTCHINSON. Yes, this is a problem that the private side does not understand well and the government understands very well yet the private side has the problem to the same degree that the government does, so this is a great opportunity for the government to inform.

Ms. ESHOO. Thank you.

Dr. Shannon?

Mr. SHANNON. Since the public is the hands that carries, you know, as you mentioned, carries out the most activity, it is the public sector's opportunity to promote trust, and that is really one of the distinguishing capabilities of our society, and as Jim Lewis has said in our venues, it is something that distinguishes us from our adversaries may approach things. So promoting trust I think is the real opportunity on the government side.

Ms. ESHOO. Thank you.

Ms. STEMPFLEY. Continue refinement in statute of the authorities of the government in a situation——

Ms. ESHOO. Excuse me. What?

Ms. STEMPFLEY. Continue refinement in statute of authorities of organizations such as the Department of Homeland Security.

Ms. ESHOO. What does that mean?

Ms. STEMPFLEY. Excuse me?

Ms. ESHOO. What does it mean?

Ms. STEMPFLEY. So what that means, ma'am, is what you find in the Department is that our authorities are spread across multiple statutes and multiple directives, and it is a bit of patchwork landscape for us and provides great——

Ms. ESHOO. Well, that is the story of DHS.

Ms. STEMPFLEY. Yes, ma'am. So if we refine that relative to statute, that will put some clarity in terms of this and enable stronger information sharing and information sharing in action.

Ms. ESHOO. Let me ask you something about this—it sounds to me like a mini NSA with the center. Do you deal with things after the fact and then you can advise Federal agencies about how a cyber threat has affected them or do you defend the workings of agencies so that they don't experience it? I am not so sure what this group does. We would like to come out and see it. Can you answer that for us? I am trying to picture it and what you do.

Ms. STEMPFLEY. I certainly can, ma'am. We do—we provide prevention information and standards for Federal executive civilian branches to follow that are about raising the security of their branch so items they must do in order to be—in order to meet the standard, and then we provide response actions when something goes wrong as well as detection and prevention activities at the boundary.

Ms. ESHOO. Well, I am over my time, and I thank all of you for not only the work you do but making that come alive here in your testimony. Thank you.

Thank you, Mr. Chairman.

Mr. WALDEN. Thank you.

We will now turn to Mr. Terry, the vice chair of the subcommittee, for questions.

Mr. TERRY. Thank you, Mr. Chairman, and I want to follow up on both of the sets of questions.

Admiral Barnett, I want to commend you for the job in CSRIC, and could you just briefly go over the main principles, the five main principles that are outlined by CSRIC?

Mr. BARNETT. There are actually major things, and I am very pleased to have with me Jeff Goldthorpe, who is our Associate Bureau Chief for Cybersecurity, who really led and put together this incredible team. So the first one was the anti-bot code of conduct for ISPs. All of these address ISPs. They are all voluntary industry based. And basically the five tenets under the anti-bot thing is education of the public so they understand what the problems are, and that obviously goes to prevention; detection when they are infected; providing notice to them that their computer is infected because most of the time they don't realize that their computer is infected, and then giving them some tools or some resources in order to get their computer cleaned and in collaboration to make sure that that information is spread across other ISPs so we're refining all this together.

And with regard to DNSSEC, it is encouragement to move forward on implementation so to make all DNSSEC servers DNSSEC aware, and on the Internet route hijacking, which as the chairman mentioned is a little bit arcane and hard to understand, but the main thing is, is establish a secure, authoritative database in which addresses can be registered so this would probably be with the American Registry of Internet Numbers. And then ISPs can actually check their routes against it and it will be authoritative. They will know where it is going. We think this will get rid of all of the misrouting and will do a lot to help us detect malicious routing. So those would be the three main things.

Mr. TERRY. All right. You mentioned a key phrase in there, voluntary and industry based. Can you tell us why it is important that standards and ways of implementing what you stated should be voluntary and industry based?

Mr. BARNETT. The FCC as a regulator actually has a long history of working with industry to come up with best practices. As a matter of fact, the FCC's NRIC, a predecessor of CSRIC, came up with the first cybersecurity best practices back in 2002. So by getting the experts together in the same room and coming up with best practices with codes like this, we think we can get a lot of things done. And it is also important as CSRIC's work continues to make sure that we have the metrics to understand, are those voluntary measures actually having the effect we want to so CSRIC's work actually continues.

Mr. TERRY. All right. Starting with you, Ms. Alexander, do you agree with those principles?

Ms. ALEXANDER. Yes. At NTIA we would very much support a multi-stakeholder approach to Internet policymaking, and it is really important that the breadth of stakeholders that are involved in the ecosystem be part of these processes.

Mr. TERRY. How about voluntary and industry does their own standards?

Ms. ALEXANDER. Yes, sir.

Mr. TERRY. Mr. Hutchinson, what do you think?

Mr. HUTCHINSON. I agree with the voluntary nature of the standards. One thing that we need, though, is better experimentation around what constitutes best practices rather than just a declaration. We need to be able to conduct experiments.

Mr. TERRY. Good point.

Mr. Shannon, you are the one non-Federal Government employee at this panel.

Mr. SHANNON. Yes. I actually participated in the 2002 NRIC discussions, so I understand the value of that collaboration. As the admiral mentioned, I agree that putting metrics on place to determine if they are being effective is appropriate. You know, take the lightest weight approach first. If voluntary compliance works, then that is excellent, and it would be wonderful to have metrics that confirm that.

Mr. TERRY. Very good.

And Ms. Stempfley?

Ms. STEMPFLEY. Thank you, sir. I believe that the innovations that industry provides and the best practices they provide are incredible useful and very vital in our success in this environment and bringing them together in a voluntary nature is very important. As we go forward with the metrics associated with those, their effectiveness and their use I think is the place where we need to——

Mr. TERRY. There is some effort by some Senators and members that state that Homeland Security should be the one developing with industry the standards for cybersecurity in the private sector. Do you agree with that?

Ms. STEMPFLEY. I believe that Homeland Security's responsibilities are building standards across critical infrastructure and working with the sector experts in each sector for standards for cybersecurity.

Mr. TERRY. How would you develop those standards?

Ms. STEMPFLEY. We would develop——

Mr. TERRY. And how would you enforce them? By rule?

Ms. STEMPFLEY. I am sorry, sir. I didn't hear you.

Mr. TERRY. Would that include developing rules then?

Ms. STEMPFLEY. I believe that we need to bring industry together in order to determine within each sector what is important and then identify where we need to put in place best practice and rules or other mechanisms for assurance of compliance with best practices.

Mr. TERRY. I would respectfully state that I disagree, and I think, frankly, putting an agency in charge of developing rules, even with collaboration, is dooming that industry. Yield back.

Mr. WALDEN. The gentleman yields back his time.

I now recognize the gentlelady from California, Ms. Matsui.

Ms. MATSUI. Thank you, Mr. Chairman.

An integral part of how the government is asking agency reform to IT purchasing involves greater use of the cloud. As the government's Chief Information Officer has said, last year agencies successfully migrated 40 services to the cloud and were able to eliminate more than 50 legacy systems in order to save taxpayer dollars while expanding capabilities. I have a question for Admiral Barnett, Ms. Alexander and Ms. Stempfley. Some of the government agencies here today are using cloud services. What can you share with us from your early experiences with regard to cyber protections and threats? Ms. Alexander?

Ms. ALEXANDER. I am actually not the Department's expert on cloud issues but I would be happy to make sure we get you an answer for the record.

Ms. MATSUI. Admiral Barnett?

Mr. BARNETT. Thank you, ma'am. So cloud services, my former colleague at FCC, Steve VanRoekel, has highlighted how valuable cloud services can be. It does emphasize the need to make sure that the transport between the user agency or company and that cloud is secure and reliable. It is another thing that we and I think the people that you see at this table are considering is what happens for continuity of operations, continuity of government, and so there is some considerations we need to make sure on that, but really it emphasizes some of the very same things that we have talked about today is the network reliability and security.

Ms. MATSUI. OK. Ms. Stempfley?

Ms. STEMPFLEY. Cloud presents some really good opportunities to get your arms around configuration management and architecting opportunities so to get at the root cause. It also has some particular threat opportunities as well, as Admiral Barnett indicated, and you have to look at it in that holistic lens as we move forward, and it is certainly a part of the government's program to do so.

Ms. MATSUI. OK. But as the private sector moves increasingly to the cloud, what challenges do you foresee?

Ms. STEMPFLEY. So I think as Admiral Barnett indicated, bringing all of the content together into a single place presents a route diversity requirement and a continuity requirement. Cloud also presents the opportunity to overcome that within the way the cloud is architected. So it is a wonderful capability for us but it is one of those where it is both a challenge and an opportunity simultaneously.

Ms. MATSUI. OK. Thank you.

Dr. Shannon, it is my understanding that there are a number of clearinghouses, area clearinghouses, that are used to store information relating to cyber threats. U.S. CERT acts as one of these clearinghouses. What is the relationship between those silos and industry and government sharing? Can any company access your clearinghouse or do they need to be a member of some sort?

Mr. SHANNON. CERT is part of an FFRDC collaboration along with NIST to create vulnerability databases, and that is a public resource that is widely available. Of course, we also participate in government-focused ones, and that is part of the policy decisions that need to be made that are part of the discussions about how to share that more broadly.

Ms. MATSUI. OK. So with multiple clearinghouses, does it make sense to have a streamlined process for information sharing for any stakeholder who is threatened with attack or at risk?

Mr. SHANNON. Anyone who is under threat or under attack needs to know where to turn to, and I think providing that clarity is part of what policymakers can help resolve. There has been times when CERT has served that purpose, U.S. CERT has served that purpose, and as Ms. Stempfley indicated, there is confusion.

Ms. MATSUI. OK. Admiral Barnett, I am pleased to hear you already have commitments from major ISPs to implement CSRIC recommendations. How do we share that with smaller companies with likely much fewer resources have the ability and incentives to do the same?

Mr. BARNETT. It is a great question, ma'am. One of the things I think you will see is that these things are going to start becoming the industry standard, reviewing a lot of flexibility for companies and how they implement them and over what time. Hopefully they can do them along with their normal business processes working with the American Cable Association or maybe the smaller systems to figure out what are the best ways, and one of the major things, as I mentioned, CSRIC's work continues. The next things that we set them on is, what are the barriers to implementation, how do we get over those. So these same great experts are going to come back together and start working on those very things.

Ms. MATSUI. So there is a concerted effort to reach out to some of the smaller companies?

Mr. BARNETT. Yes, ma'am.

Ms. MATSUI. OK. That is great. Good.

Let me see. Dr. Shannon, in your testimony, you stress the importance of secure coding so initiatives such as addressing root causes of cyber threats. Is this concept applicable to apps that are downloaded to mobile devices that connect to the Internet such as smartphones and our tablets?

Mr. SHANNON. Yes. It is highly applicable. I mean, there is two parts of the app's development environment. One is the infrastructure and that needs to be coded securely. Fortunately for the app developers, there is a more constrained environment so it is a possibility for the ecosystem owner to help protect the users and to ensure that the app developers are developing appropriate apps. But part of it is, is that, you know, we will find vulnerabilities there and that is how you train, you know, the teenagers that are writing the apps to write them correctly. I mean, it is a serious challenge but, you know, it is that balance with innovation.

Ms. MATSUI. Sure. OK. Thank you very much.

Mr. WALDEN. You hire them at Sandia Labs.

We will go now to the gentlelady from California, Ms. Bono Mack, for questions.

Mrs. BONO MACK. Thank you, Mr. Chairman.

Ms. Stempfley, I can't see you over there, but my first question is directed to you. Since Congress created the Chemical Facility Antiterrorism Standards, or what we call CFATS, program in 2007, there have been ongoing problems with the way DHS has managed the program. These problems include DHS improperly tiering 600 chemical facilities, wasteful spending and the inability of DHS to properly train the workforce responsible for carrying out the chemical security program. Hundreds of millions have been spent on CFATS. We find ourselves with a program that has been mismanaged, wasted taxpayer dollars, and no assurance that our chemical facilities are in fact secure.

Can you tell me with these significant problems in the instance of CFATS how you could possibly assert to this committee that DHS will not mismanage cybersecurity?

Ms. STEMPFLEY. Ma'am, thank you very much for the opportunity to address that. The differences between chemical facilities and information technology and communication are fairly profound in that situation, and so as we work as a department of experts brought together and engage in these discussions with industry about what are the basic standards that are necessary, we envision building those basic standards in that scenario and then learning lessons across the Department from areas where we have worked through issues. We want to ensure that we don't make the same mistakes a second time.

Mrs. BONO MACK. With all due respect, I didn't really hear an answer in your answer, but I would say to you that perhaps there are differences between chemical facilities and cybersecurity yet I think from the American people's point of view, it is the bureaucracy, and I think you have rattled off quite a list of acronyms but I don't know that my constituents would feel safer by the list of acronyms that you have used. In fact, to me, did I mishear you? The example of the EDA's Web site or network being down for weeks when you were asked a question by the chairman, you know, what do you and you are responsible for prevention and mitigation. Is that not an example, though, of failure of all of these bureaucracies to in fact work together well?

Ms. STEMPFLEY. The example presented by the chairman, ma'am, with Commerce is an example where we in the Department and the Department of Commerce have joint action that must be taken. So in that scenario, the Department of Commerce has the responsibility for the management and security of their systems in building them and in operating them following the standards set by the Department of Homeland Security.

Mrs. BONO MACK. Thank you.

To Admiral Barnett, you know, I agree that the Federal Government should be involved in our country's cybersecurity efforts, absolutely, but they should be enhancing cooperation and they should be the facilitator, not a regulator. Can you elaborate a little bit on your thoughts on the value of a cooperative relationship with the private sector versus a regulatory one?

Mr. BARNETT. Yes, ma'am. So certainly the CSRIC actions last week are an example of that, but there are many, many others. CSRIC also addresses cooperation in the telecommunications industry on next-generation 911, on emergency learning, and as Dr. Shannon mentioned, we have done this for years and years. I think it is helpful when you have the regulator who is the expert in the United States to be involved with this. They will sit down with industry, just like the experts that I mentioned that I brought with me today. We have experts in other areas like the ones I have mentioned in next-generation 911, to be able to sit down with industry to pull them together, and quite frankly, that is one of the reasons that we were able to pull together these experts to come up with voluntary industry-based solutions.

Mrs. BONO MACK. Thank you. I think my biggest concern is recognizing how quickly the cyber world knows and the bad guys are by nature one step ahead of the good guys, so the question really is, with all of the regulatory hurdles potentially, how do we really keep pace with the threat?

Mr. BARNETT. Yes, ma'am. So recognizing that the large majority of telecommunications cybersecurity are in private hands, there is a couple things to that. They are the first lien of defense. Our actions, and I think what you have heard mostly from these panelists, is to enhance those but we also have to recognize something else. It is not working. We wouldn't be here concerned about this if that was enough, and so as Dr. Shannon mentioned, we have to have metrics to make sure that the voluntary methods that we are employing work, and then beyond that to look at whatever else. Hopefully there would be other things that we could do, so information sharing is one thing. There may be other best practices that we can do. But the thing that is an absolutely prerequisite on this is, we have to make sure that they are effective because we cannot go on any longer the way we are now.

Mrs. BONO MACK. Thank you. My last question, and then I am out of time. To any of you, are government agencies able to effectively combat cyber agitators that we are very well aware of right now like Anonymous and WILSEC and what are we doing to stop their attacks. To anybody I will pose that question and then I am out of time.

Ms. STEMPFLEY. Government departments and agencies every day are working to defend against threats as you indicated both in terms of Anonymous and WILSEC, and in the instance where they have been unsuccessful, we work in partnership to help them overcome the impacts of those attacks in that situation through a layered defense strategy which includes things like the Einstein program and things like the establishment of standards through the Federal network security programs.

Mr. SHANNON. I would say just briefly, I would encourage you to talk to the law enforcement community. I think they have been doing a very effective job given some of the recent arrests in that area.

Mrs. BONO MACK. All right. Thank you, Mr. Chairman, for the time and I yield back.

Mr. WALDEN. The gentlelady yields back, and Admiral Barnett, we agree with you on the accountability and matrix and all that.

Mr. Dingell for 5 minutes.

Mr. DINGELL. Thank you, Mr. Chairman. I hope you are not still smarting from yesterday's handling of that legislation.

Good morning. This first question will be to all witnesses yes or no. Ladies and gentlemen, industry witnesses told this subcommittee on March 7, 2012, that the Federal Government would facilitate better interindustry and public-private information sharing. Do you agree with that opinion? Yes or no, starting with Ms. Alexander.

Ms. ALEXANDER. Yes.

Mr. DINGELL. Admiral?

Mr. BARNETT. Yes, information sharing can be a government role.

Mr. DINGELL. Just yes or no, because I am running out of time.

Mr. HUTCHINSON. Yes.

Mr. SHANNON. Yes.

Mr. DINGELL. Ma'am?

Ms. STEMPFLEY. Yes.

Mr. DINGELL. Good. Again, to all witnesses, again, yes or no. Senator Lieberman's cybersecurity bill, S. 2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Yes or no.

Ms. ALEXANDER. Yes.

Mr. DINGELL. Admiral, they don't have a nod button. You have to say yes or no.

Mr. BARNETT. Yes.

Mr. DINGELL. All right. Next witness.

Mr. HUTCHINSON. Yes.

Mr. SHANNON. No comment.

Ms. STEMPFLEY. Yes.

Mr. DINGELL. Thank you. Now, this is for all witnesses. Similarly, do you believe promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber threats? Yes or no. Ms. Alexander?

Ms. ALEXANDER. No.

Mr. DINGELL. Admiral?

Mr. BARNETT. No.

Mr. DINGELL. Next witness.

Mr. HUTCHINSON. Yes.

Mr. DINGELL. Next witness.

Mr. SHANNON. It is a risk.

Mr. DINGELL. Next witness.

Ms. STEMPFLEY. No.

Mr. DINGELL. All right. Now, Admiral Barnett, you mentioned in your testimony the Communications Security, Reliability and Interoperability Council—that is CSRIC—recommendations about preventing domain name spoofing, route hijacking and botnet attacks. These recommendations are voluntary, are they not?

Mr. BARNETT. Yes, sir.

Mr. DINGELL. Now, again, Admiral, how many Internet service providers—ISPs—have adopted CSRIC's recommendations?

Mr. BARNETT. There are nine Internet service providers that have pledged to implement those recommendations.

Mr. DINGELL. Out of how many?

Mr. BARNETT. Well, there are literally thousands, I guess, when you start talking about the small cable operators, and we are working with the various associations——

Mr. DINGELL. So what you are telling me is, you have a penetration of nine out of thousands?

Mr. BARNETT. Well, we have a penetration that will cover 80 percent of American Internet users right from the beginning and we will continue to go towards 100 percent.

Mr. DINGELL. Of course, if they can shut down your banking industry, they can shut down your electrical utility industry, your handling of your net, they could shut down the natural gas pipeline system in this country, refineries, auto companies, God knows what else they can shut down with that kind of opportunity available.

Mr. BARNETT. That is why we are going to continue to work for 100 percent.

Mr. DINGELL. When will you hit 100 percent? Do you have any idea?

Mr. BARNETT. We don't at this particular point but I felt pretty good about getting 80 percent commitment from the beginning, and we are going to continue work on the barriers to implementation so that we can get even the smaller Internet service providers as soon as possible.

Mr. DINGELL. All right. Now, to all witnesses, similarly, can and should CSRIC's recommendations be adopted by the FCC or other Federal agencies and thereby be made mandatory? Please answer yes or no, but I would very much appreciate a written submission explaining your comment, starting with you, Ms. Alexander.

Ms. ALEXANDER. No.

Mr. DINGELL. Admiral?

Mr. BARNETT. No, sir.

Mr. DINGELL. Next witness.

Mr. HUTCHINSON. No.

Mr. SHANNON. Only when there is supporting data.

Mr. DINGELL. Next witness.

Ms. STEMPFLEY. No, sir.

Mr. DINGELL. Thank you. And please submit that. I am sorry to do that to you but the time here is rather limited.

Ms. Alexander, your testimony focused largely on domain name security extensions. As you know, Internet Corporation for Assigned Names and Numbers, ICANN, has signaled its intention to increase by many fold the number of generic top-level domain names. Is NTIA concerned that such expansion may complicate efforts to deploy DNSSEC as well as compromise DNSSEC's future effectiveness? Yes or no.

Ms. ALEXANDER. No, sir, it is a requirement.

Mr. DINGELL. Would you submit an appropriate further response on that matter?

Ms. ALEXANDER. Absolutely.

Mr. DINGELL. Now, other witnesses, do any of you, starting with you, Admiral, care to comment on Ms. Alexander's comments?

Mr. BARNETT. No, sir.

Mr. DINGELL. Next witness.

Mr. HUTCHINSON. No comment.

Mr. DINGELL. Next witness.

Mr. SHANNON. Any technology that hasn't been deployed for decades may potentially have vulnerabilities, and that is always a fundamental challenge in the age of the Internet. There are unforeseen uses decades down the road. Leading academics have contributed to DNSSEC. It is one of our best efforts to try and tackle these issues, so I am confident that it will stand the test of time.

Mr. DINGELL. Ms. Stempfley?

Ms. STEMPFLEY. No comment.

Mr. DINGELL. Thank you.

Thank you, Mr. Chairman, for your courtesy.

Mr. WALDEN. Thank you.

We will now go to Ms. Blackburn for 5 minutes for questions.

Mrs. BLACKBURN. Thank you, Mr. Chairman, and I want to thank all of you for your time and for being here.

Mr. Hutchinson, I want to come to you first and ask you about the program that you all have that you liken to a medical residency in cybersecurity. So what I would like to know is how that is structured, if you could give us a little bit more detail. Is it public-private partnership? And the reason I ask this is because in the area that I represent in Tennessee, there around Nashville, we have so many individuals that started working on the entertainment industry platforms and they have moved to defense informatics or over to health care informatics and then some of them are in financial service informatics, and we see so much sharing on the skills that are there to keep the backbone of the Internet safe, if you will, and I think it is fascinating that you all have done something, but as we talk about having a trained workforce who is able to handle this, it sounds like a good idea and I would love a little detail if you are able to share that.

Mr. HUTCHINSON. Yes. Thank you for that question. What we realized is that technology is nowhere near ready to protect our networks, that it really requires people and it requires creative people who can adapt to lots of technology and tools. When we built this program, we focused on bringing the participants together in a common environment, to carefully pair those individuals and team them with mentors, and to create——

Mrs. BLACKBURN. Let me stop you right there. How do you select individuals for this program? How do you pick them out and select them?

Mr. HUTCHINSON. OK. So in the early days, we selected them through an application and résumé and interview process. Today, there is a lot of referrals, so we get referrals from people who understand this program, and so we place them in this environment. They work together on teams. They work on actual national security problems. They learn security through that experience. They learn all the balances and the gives and takes and what makes cybersecurity particularly difficult, and as they build these projects out and make these tradeoffs, they just gain the type of instinct that a medical student must also gain in a residency program.

Mrs. BLACKBURN. OK. That sounds great. Now, any of the graduates of your program, if you will, and I use that just as a term to kind of look at those that have come through, how many have come through the program?

Mr. HUTCHINSON. So I can provide an exact number for the record but it is about 500.

Mrs. BLACKBURN. OK. That sounds wonderful. Have any of them been helpful going forward in identifying risk or threats to the system or maybe writing programs that help to foil any of the threats? What kind of participation and results are you seeing?

Mr. HUTCHINSON. So the people who have been through this program are distributed to industry, they are in government service, they work for national labs and other FFRDCs, and there are many cases where they have developed tools that were able to identify a particular breach of a network or to develop algorithms that can provide things like directions toward attribution and criminal investigation, digital forensics capability. There is a long list of achievements.

Mrs. BLACKBURN. So you are seeing solid results?

Mr. HUTCHINSON. Solid results from these individuals.

Mrs. BLACKBURN. OK. That sounds great.

This is something I would like to hear from each of you, and I only have 1 minute left. As I mentioned earlier, we are working on cybersecurity legislation, and the question that always come up is, how narrow do you make it or how broad. And I have appreciated hearing your testimonies today. So how narrowly or broadly should Federal legislation define what can or cannot be shared between governments and private entities and should there be specific requirements on PII about innocent consumers being taken out of data packets before it can be shared with any other government agencies?

Mr. SHANNON. I encourage you to consider legislation that is broad in the sense of supporting people who need to do the right thing in response to incidents. In terms of more prescriptive approaches, I encourage you to use data-driven, you know, pilots essentially to verify that a policy that is being considered that may be prescriptive is actually going to be effective.

Mrs. BLACKBURN. OK.

Ms. STEMPFLEY. I would like the opportunity to come back to you via technical assistance or others and describe the processes we use in the Department today for how to protect privacy and other considerations where what we are mostly focused on are indicators, the specific technical pieces of information that are useful. While it is not possible to always avoid in that indicator selection of some things that may be of concern, we have strong protection measures in place to ensure as we are working to get to the indicators the malicious code, so I would like to follow up.

Mrs. BLACKBURN. Thank you. I appreciate that. I yield back.

Mr. WALDEN. I thank the gentlelady and now I turn to Mr. Stearns for final questions.

Mr. STEARNS. Thank you, Mr. Chairman. I think maybe you heard my opening statement talking about Shawn Henry, the FBI's top cyber cop, and so I was going to ask each of you starting with you, Ms. Alexander, Mr. Henry told the Wall Street Journal that we are not winning the cybersecurity battle. He went on to say "We have been playing defense for a long time, and you can only build a fence so high, and what we found is that the difference that the offense outpaces the defense and the offense is better than the defense. Do you agree or disagree with the assessment of Shawn Henry?

Ms. ALEXANDER. Thank you very much, Congressman. I am not familiar with the article or what he said but I would say he just points to the reason why we are here today and why we are all working so closely across the Federal Government to be vigilant dealing with these issues.

Mr. STEARNS. Admiral?

Mr. BARNETT. Yes, sir, I would agree with him. We cannot sustain the way it is going right now. We have too much of our economy that is now invested in ones and zeros. There are so many other things, verticals, critical infrastructures, that depend on our communication infrastructure to impact it. So we have to take action, and so I think what you have heard here today is a call for that. And in answer to your response, we appreciate this hearing to focus on it.

Mr. STEARNS. Mr. Hutchinson?

Mr. HUTCHINSON. Attackers do have an easier job than a defender has, and that is problematic, and it is resource-depleting. I completely agree with the assessment that the defenders are on the wrong side economically. I mean, it is very easy for an attacker to attack a system and cause a lot of money to be spent in defending that system. But the solution is to accept that our networks will never be free of compromise and to find ways that we can operate in the face of compromise, and that is an open research challenge. There is certain progress in that direction and I would encourage additional support for those forms of research objectives.

Mr. STEARNS. Dr. Shannon?

Mr. SHANNON. It is a dramatic article. I have not read it. It is certainly the sort of articles that we have seen for many decades in the area of cybersecurity. They just tend to get more press these days.

You know, I would encourage you to remember that it is about root causes versus innovation. You know, we all received email this morning, the sky isn't falling. There are serious, serious challenges but it is easy to get a little carried away, in my view.

Mr. STEARNS. So would you agree with him or not?

Mr. SHANNON. I don't think it is just going to be so dramatic.

Mr. STEARNS. OK.

Mr. SHANNON. That is my personal opinion.

Mr. STEARNS. I appreciate your honesty here.

Mr. SHANNON. After being with colleagues who were dramatic, you know, 20 years ago about these issues.

Mr. STEARNS. OK. Ms. Stempfley?

Ms. STEMPFLEY. Thank you, sir, and thank you for the opportunity with this hearing because I think the thematics of that article are certainly what we are talking about today, and as I said, there is no single solution in this situation, and so if the premise of the article is that we need to make changes in order to increase awareness and importance of the cybersecurity challenges, then I would agree with that.

Mr. STEARNS. OK. Admiral Barnett, I think you told Ms. Eshoo earlier that we need to focus on supply chain vulnerabilities. I had a hearing as chairman of the Oversight and Investigations Subcommittee yesterday just on that with the Department of Energy, and frankly, they are doing catch-up. CBO had a report that came out mentioning that the Department of Defense and the DOE admit that they just started looking at ways to look at cybersecurity in the supply chains. So I just wonder if you had anything you would like to elaborate on on the supply chain vulnerabilities.

Mr. BARNETT. Well, at the FCC we have been looking at this for the 2 years that I have been there, and I know we have been working with other governmental partners on this. One of the things that is apparent as we look across the authorities for whatever else you can say about it is the authorities that we have right now were not designed to address the supply chain challenges we have right now, so additional work needs to continue. There are a couple of approaches that I hear going on. One is a kind of a transactional approach. One I think I am intending to favor better right now is a supply chain risk management where it is a tiered approach, and the most critical elements of our communications network are provided the most protection. That allows a little bit more flexibility as you go down to the other tiers. There are a lot of tools that are available to us that may include various supply chain standards. The government needs to work together on this to pull together and we can't start soon enough.

Mr. STEARNS. Mr. Hutchinson, according to your president and director, Paul Hommert, Sandia National Laboratories have been attacked up to 30,000 times per hour. Do some of these attacks get through your safety net? Does Sandia National Laboratories currently have supply chain checks in place with equipment that you buy?

Mr. HUTCHINSON. OK. The attacks that lab Director Hommert is referring to are not supply chain attacks per se but just operational attacks against our cyber networks and they are measured that way because we have successfully identified that as an attack and stopped it before it affected our systems. And that said, we have instances where we detect compromises that occurred on our systems and we investigate and address those as we discover them. And yes, we do have very careful supply chain processes that we follow because our prime mission of building weapons has been a victim or has been a target, not a victim, a target of supply chain attacks for many years. So we have developed our end-sharing and science capabilities to address those issues.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. WALDEN. I thank the gentleman for his questions.

Seeing no other members to ask questions, thank you very much for your testimony, for your answers to the questions, and the good work you are doing to make America safer and more secure. We appreciate it in this role and in other roles that you have had. And I thank the subcommittee members for their participation. We will continue on this topic, although I don't see future hearings at the moment planned, but we will be in contact with you, and I know some of our colleagues have questions for you to follow up on, so we appreciate your written responses to those and any other suggestions you have for us. We want to get this right, and there is too much at stake not to.

So we appreciate your help and I appreciate the participation of the committee, and with that, we stand adjourned.

[Whereupon, at 11:38 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and
Information Administration
Washington, D.C. 20230

JUL 25 2012

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives
Washington, DC 20515

Dear Chairman Walden:

Thank you for the opportunity to testify on March 28, 2012 before the Subcommittee on Communications and Technology at the hearing entitled "Cybersecurity: Threats to Communications Networks and Public-Sector Responses." I appreciate your forwarding additional questions for the record to me on June 11, 2012.

My responses to the questions are enclosed. If you or your staff have any additional questions, please do not hesitate to contact me or James Wasilewski, NTIA's Director of Congressional Affairs, at (202) 482-1840.

Sincerely,

Fiona Alexander
Associate Administrator
Office of International Affairs

CC: The Honorable Anna Eshoo, Ranking Member
Subcommittee on Communications and Technology

Enclosure

Responses to Question from the Honorable Anna Eshoo

1. **As you describe in your testimony, NTIA utilizes a multi-stakeholder process to enhance DNS security. In other areas, stakeholders are exploring ways to enable information sharing and best practices development. Were there lessons learned from the DNSSEC process that would be helpful to establishing additional multi-stakeholder processes?**

The approach taken by the Department of Commerce (NTIA and the National Institute of Standards and Technology), in cooperation with its root zone management partners (the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign), relies upon repeated multistakeholder input and involvement. For example, the Department utilized public comment mechanisms such as Notices of Inquiry, which sought community input in an open and transparent manner. In addition to these formal processes, the Department's root zone management partners sought input from the technical community. This included requests for comment on draft documentation as well as open consultations alongside meetings of the Internet Engineering Task Force (IETF), ICANN, and the regional network operations groups (NOGs). NTIA's willingness and commitment to actively seek stakeholder input was the key to the success of DNSSEC implementation at the root and one that would be helpful in establishing additional multistakeholder processes.

Responses to Questions from the Honorable John D. Dingell

1. **Your testimony focuses largely on Domain Name System Security Extensions (DNSSEC; pronounced "DNS-Seck"). As you know, the Internet Corporation for Assigned Names and Numbers (ICANN) has signaled its intention to increase by many fold the number of generic top-level domain names (gTLDs). Is NTIA concerned that such expansion may complicate efforts to deploy DNSSEC, as well as compromise DNSSEC's future effectiveness? Please explain your response.**

NTIA believes that the new gTLD expansion will in fact have a positive effect on the deployment of DNSSEC as all new gTLDs are required to implement DNSSEC. This requirement will spur further implementation and provide additional incentive for Internet Service Providers (ISPs) and other resolvers to implement DNSSEC as well.

2. **Industry witnesses told this Subcommittee on March 7, 2012, that the federal government should facilitate better intra-industry and public-private information sharing. Do you agree with that opinion? Please explain your response.**

Yes. In May 2011, the Administration submitted its proposal for comprehensive cybersecurity legislation, and has been working closely with Congress to enact those principles into law. The Department of Commerce agrees that these proposals are critical to enhancing cybersecurity, and my colleagues at the Department have been working to achieve that goal. In addition, through its Internet Policy Task Force, the Department of Commerce has focused its efforts on developing public policies and voluntary private sector norms that could improve the overall cybersecurity of private sector infrastructure operators, software and service providers, and users outside the critical infrastructure. NTIA believe that intra-industry and public-private information sharing must be an integral part of a comprehensive cybersecurity solution, with appropriate safeguards for privacy and civil liberties.

3. **Senator Lieberman's cybersecurity bill, S. 2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Please explain your response.**

Yes. In its May 2011 cybersecurity proposal, the Administration supported certain cybersecurity regulatory authorities to better protect the most critical infrastructure on which this country relies. The Department of Commerce agrees that some regulatory authority is necessary to better protect this limited class of infrastructure, while preserving the ability for owners and operators to have sufficient flexibility to meet their business needs. By proposing an approach that would involve collaboration with industry, NTIA believes that S. 2105 would effectively enhance cybersecurity while protecting commercial interests.

4. **Similarly, do you believe the promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber-threats? Please explain your response.**

No. Performance requirements would only pertain to a limited set of critical infrastructure on which the country relies. The requirements would allow industry flexibility to choose how to best meet them if current practices are not already sufficient. Furthermore, the process created by S. 2105 would require that performance requirements be developed collaboratively with industry in an open and transparent process. This would allow practices to be developed and shared that could be broadly adopted throughout industry.

5. **Can and should CSRIC's recommendations be adopted by the FCC or other federal agencies and thereby be made mandatory? Please explain your response.**

NTIA does not believe that CSRIC recommendations should be made mandatory for a number of reasons. NTIA supports the multistakeholder approach for addressing Internet policy issues. We participate in international multistakeholder processes to ensure that the Internet continues to be governed in an open and transparent manner, and that innovation continues to flourish at Internet speeds. NTIA believes that multistakeholder processes are better able to address policy questions that arise in the rapidly-changing Internet environment. Further, in order to be successful and effective, standards and practices must be adopted by a wide range of national and global stakeholders.

The U.S. government has long sought to avoid imposing technical standards on dynamic environments like the Internet, and imposing CSRIC standards would run counter to that strong principle. Moreover, doing so would set a very problematic precedent for the rest of the world, just as the United States is resisting other countries' efforts to impose greater governmental control over the Internet.

Finally, as NTIA embarks upon its multistakeholder processes in the privacy area, we are concerned that mandating CSRIC recommendations would undermine stakeholders' willingness to engage in government-convened dialogues regarding important Internet policy topics. The CSRIC recommendations at issue here were crafted – primarily by industry – on the understanding that they would be used as voluntary best practices. To take those recommendations and make them mandatory after the fact would undermine industry's willingness to participate in government-convened dialogues to address policy issues in the future.

Responses to Question from the Honorable Bob Latta

1. **In your testimony you talk about the role NTIA has taken to facility [*sic*] greater DNS-SEC deployment, and that for the greatest benefits of DNS-SEC, there needs t be broad deployment. One thing I have learned from our cybersecurity hearings is that new threats are always emerging—do we get to the point where DNS-SEC can easily be infiltrated?**

Like all systems, it is important that organizations maintain proper cybersecurity operations to minimize the risk of being infiltrated. In the area of DNSSEC, it is critical that organizations ensure they have the proper operations (*i.e.*, patching, key changes, and more) in place to minimize the risk.

Federal Communications Commission
Office of Legislative Affairs
Washington, D.C.20554

Office of the Director

June 25, 2012

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Walden:

Attached please find responses to the post-hearing questions from the hearing on "Cybersecurity: Threats to Communications Networks and Public-Sector Responses" held on March 28, 2012. Please note that Admiral Barnett has left the Commission since his appearance at the hearing.

Sincerely,

Gregory W. Guice
Director

House Committee on Energy and Commerce
Subcommittee on Communications and Technology
Hearing on
"Cybersecurity: Threats to Communications Networks and Public-Sector"
Responses of Federal Communications Commission to Questions for the Record

The Honorable Anna Eshoo

1. **What challenges do you expect smaller ISPs will face in adopting the industry best practices recommended by CSRIC?**

Response: Because the process for adopting industry best practices is voluntary, smaller ISPs have the flexibility to proceed with implementation in a way and on a schedule that meets their particular needs. Compliance becomes easier and cheaper as best practices become more widely adopted. One benefit from the recommendations not setting an implementation date is that smaller ISPs are at liberty to implement the best practices consistent with their normal business processes and timetables. They can also draw on the knowledge and experience of companies and associations that have already adopted or focused closely on the best practices, including organizations that represent smaller ISPs.

CSRIC is continuing its work and is making a concerted effort to address the unique needs of smaller ISPs. For example, a CSRIC Working Group has assembled an impressive set of practitioners to address barriers to implementation and how to overcome them.

2. **What is your view of the communications supply chain risk, and how can we best address this concern?**

Response: The Commission has been working with other governmental partners on this important issue. Because its own authority was not originally designed to address supply chain risk challenges, it could be appropriate to explore changes.

Separately, a number of experts have suggested a tiered approach to the Commission to address supply chain issues, in order to mitigate risk at a tolerable cost. Under this approach, government involvement would increase with the level of risk. Only the most critical elements of our communication networks would be provided the most protection, allowing for a less costly approach for less critical tiers.

Federal partners have a number of tools with which to address a potential supply chain threat and to consider adoption of various supply chain standards. Any comprehensive solution would require coordination among several agencies of government.

The Honorable John D. Dingell

1. **You mention in your testimony the Communications Security, Reliability, and Interoperability Council's (CSRIC; pronounced "Scis-rick")**

recommendations about preventing domain name spoofing, route hijacking, and botnet attacks. Are those recommendations are (sic) voluntary?

Response: Yes.

2. **How many Internet Service Providers (ISPs) have adopted CSRIC's recommendations?**

Response: Nine ISPs covering roughly 86% of American Internet users have already pledged to implement the CSRIC recommendations. We will continue to work on any obstacles to, and to promote, voluntary adoption of these recommendations in order to achieve 100 percent adoption.

3. **You mention in your testimony that you "[...] hope more ISPs will adopt these measures." Would you please submit for the record why you believe other ISPs might not adopt CSRIC's recommendations?**

Response: We cannot speak to why ISPs may or may not adopt the recommendations, but the increased implementation of these standards creates momentum toward 100% adoption. CSRIC is continuing its work and is making a concerted effort to address the unique needs of smaller ISPs. For example, a CSRIC Working Group has assembled an impressive set of practitioners to address barriers to implementation and how to overcome them.

There is a concerted effort to address the unique needs of smaller ISPs that have not yet pledged to implement the recommendations.

4. **Industry witnesses told this Subcommittee on March 7, 2012, that the federal government should facilitate better intra-industry and public-private information sharing. Do you agree with that opinion? Please explain your response.**

Response: Yes. Information sharing is a very important tool to address the threat of cyber attacks. Initiatives like CSRIC bring industry stakeholders together in a forum that facilitates sharing of information between practitioners in an environment of trust. We believe public/private ventures like CSRIC are vital to the smooth flow of information among service providers that are on the front-lines of cybersecurity.

5. **Senator Lieberman's cybersecurity bill, S. 2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Please explain your response.**

Response: We have not taken a position on the various legislative proposals in Congress concerning cybersecurity. In assessing the proper role of government in cybersecurity, key principles include: preserving the multi-stakeholder model; enabling stakeholders across the ecosystem to work together and develop practical solutions to secure our networks; facilitating smart, practical, and voluntary solutions through cooperative efforts to achieve cybersecurity; and enabling Federal partners to work closely together in a whole-of-government approach.

6. **Similarly, do you believe the promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber-threats? Please explain your response.**

Response: See Response to Question 5.

7. **Can and should CSRIC's recommendations be adopted by the FCC or other federal agencies and thereby be made mandatory? Please explain your response.**

Response: The Commission has a long history of working with industry to develop voluntary best practices. For example, the FCC's NRIC, a predecessor of CSRIC, came up with the first cyber-security best practices back in 2002.

Nonetheless, it is important to confirm whether CSRIC's voluntary best practices are actually having their desired effect. Toward that end, outcome-oriented performance metrics should be used to assess success.

<u>**The Honorable Bob Latta**</u>

I'd like to hear a little more about the Code of Conduct developed by CSRIC (pronounced cisrec). What did that process involved (sic) and how are you encouraging ISPs to participate?

Response: The Cybersecurity and Communications Reliability Division was formed in 2009, and augmented the PSHSB's cybersecurity and communications capabilities. This division helps coordinate the work of our federal advisory committee, the Communications Security, Reliability, and Interoperability Council (CSRIC)

The CSRIC is now made up of over 50 leaders from the private and public sectors, including cyber experts from DHS and NIST and a veritable all-star cast of Internet pioneers and world class cybersecurity experts.

In March 2011, Chairman Genachowski tasked the CSRIC with developing best practices to help address major Internet security vulnerabilities. The Chairman identified three areas where action is required to better protect commercial communications networks:

1. Securing the Domain Name System (DNS) to prevent spoofing and DNS cache poisoning;
2. Improving the security of Border Gateway Protocols to prevent Internet route hijacking; and

3. Defeating botnets that cause distributed denial of service attacks and pilfer private information and money.

In March 2012 the CSRIC approved voluntary, industry-based recommendations addressing all three critical problems.

The Commission has a long history of working with industry to develop voluntary best practices. For example, the FCC's NRIC, a predecessor of CSRIC, came up with the first cyber-security best practices back in 2002.

Bob Hutchinson
Senior Manager for Information Security Sciences
Sandia National Laboratories

June 21, 2012

The Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
The Honorable Anna Eshoo
Ranking Member, Subcommittee on Communications and Technology
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C., 20515-6115

Subject: Responses to questions for the record from the House Committee on Energy and Commerce, following up on the March 28, 2012 hearing entitled *"Cybersecurity: Threats to Communications Networks and Public-Sector Responses"*

Dear Chairmen Walden and Ranking Member Eshoo:

Thank you for the opportunity to testify at your March 28, 2012 hearing on cybersecurity, and for the opportunity to address the additional questions for the record posed in your letter of June 11, 2012. My responses to the questions for the record are included below. Please contact me anytime should you have further questions or seek further discussion of these matters.

I will begin by making the point that my responses represent my own personal beliefs, and do not necessarily represent the position of Sandia National Laboratories[1] or the U.S. Department of Energy.

Responses to Questions from The Honorable Anna Eshoo

1. **You address supply chain issues in your testimony, suggesting that the government can help by informing industry of lessons learned. How in your opinion can this best be accomplished?**

   Government can help inform industry of lessons learned because some sectors of the federal government have been forced, due to the nature of their missions, to address supply chain issues over the past several decades. These sectors include the nuclear weapons complex and the intelligence community, both of which have developed a number of experts in supply chain integrity. The government could utilize these

[1] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

experts to develop a set of product development and acquisition recommendations that industry could use to aid in decision making. For example, through this expertise, government can help the private sector adopt a mindset of vulnerability assessment at points of quality assurance within their existing supply chain processes. This mindset can lead to the rapid development of training and tools that will enable industry to better ensure the integrity of their products.

2. **Your cybersecurity research brochure states, "in order to gain confidence that a cyber system performs in a secure and trusted manner, it must be analyzed, tested, and independently validated." What percentage of organizations properly test their systems? What's preventing 100 percent of organizations from doing so?**

   I do not have access to broad statistics on organizations' testing practices, and cannot comment on the percentage of organizations that properly test their systems.

   The large operating system vendors have clearly instituted effective testing and analysis programs. While these efforts can never eliminate vulnerabilities in complex systems, they can raise the cost to adversaries by making it much more difficult to discover exploitable vulnerabilities. I would note that as this trend continues, sophisticated adversaries will have increased incentives to turn their attention to supply chain exploitation. Smaller vendors of software applications continue to deliver products with a high occurrence of exploitable vulnerabilities. Because large and small vendors operate together on a single system, these vulnerabilities diminish the security advances of the larger vendors. What prevents smaller vendors from establishing highly effective testing and analysis programs? I would contend that a limited supply of qualified security experts along with business models that require rushing products to market are the main factors.

<u>Responses to Questions from The Honorable John D. Dingell</u>

1. **Industry witnesses told this Subcommittee on March 7, 2012, that the federal government should facilitate better intra-industry and public-private information sharing. Do you agree with that opinion? Please explain your response.**

   The government's role in facilitating intra-industry information sharing should focus on ensuring that industry players do not fear negative legal consequences resulting from their sharing security-related information. With that assurance in place, it is my belief that industry players will determine that it is in their best interests to share security information. The government can promote public-private information sharing in two ways:

   1) Many industry actors have important impacts on national security, and the government must facilitate sharing of those organizations' security information with national security officials so those officials can properly assess and address broad national security needs. The key to facilitating this

sharing will be to demonstrate that the government can maintain confidentiality and that industry actors will not be penalized for sharing information.

2) The government must work to inform industries that have a national security impact of threats and lessons learned by government in information security. Likewise, some industry players have, like the government, faced unique security challenges, and their lessons learned would be valuable to national security officials.

2. **Senator Lieberman's cybersecurity bill, S.2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Please explain your response.**

   If critical infrastructure owners do not have proper incentive to secure their systems, it is incumbent on the government to understand the reasons before moving to regulation. In this case, the government could instead help critical infrastructure owners voluntarily make the right security decisions through information sharing programs. Second, requirements levied for one industry or company may be wrong for another, and by implementing industry requirements the government could contribute to new security concerns that otherwise may not have existed.

3. **Similarly, do you believe the promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber-threats? Please explain your response.**

   I believe that by levying security requirements, government implicitly encourages industry to meet only those minimum requirements and go no further. Additionally, the slow pace of policymaking as compared to the rapid development of new technologies likely would render any performance requirements irrelevant in a short matter of time.

4. **Can and should CSRIC's recommendations be adopted by the FCC or other federal agencies and thereby be made mandatory? Please explain your response.**

   While I am not qualified to address the CSRIC recommendations specifically, as detailed in my prior answers I do not believe mandatory regulation will address the threats that we face.

Dr. Gregory E. Shannon, Chief Scientist for the CERT Program at The Software Engineering Institute at Carnegie Mellon University

Response to Questions for the Record pertaining to the House Committee on Energy and Commerce, Subcommittee on Subcommittee on Communications and Technology hearing: "Cybersecurity: Threats to Communications Networks and Public-Sector Responses" on March 28, 2012

The Honorable Anna Eshoo
What steps can we take to encourage more computer science and engineering majors to seek careers in cybersecurity?

One way to engender this growth is by supporting the Federal Scholarship For Service (SFS) program (https://www.sfs.opm.gov/). Growing the SFS program would add sorely needed talent to the federal workforce; and ensure that federal cyber workers were properly trained and educated. Another option would be to expand the sponsoring facilities for the Science, Mathematics, And Research for Transformation (SMART) Scholarship for Service Program to FFRDCs and even more federal labs (http://smart.asee.org/).

The Honorable John D. Dingell
1. Industry witnesses told this Subcommittee on March 7, 2012, that the federal government should facilitate better intra-industry and public-private information sharing. Do you agree with that opinion? Please explain your response.

Yes. Furthermore, we would support a non-government entity to facilitate such sharing.. Experience has demonstrated that the non-governmental community (whose participation is vital) is more comfortable sharing information with another non-government entity. Furthermore, requiring private companies to provide data to the government will likely create compliance-driven information sharing which leads to the bare minimum disclosure of sensitive information related to problems, concerns, and vulnerabilities (and often not in time to take the necessary actions). We believe that a "third-party, honest broker" facilitator for the disclosure, analysis, and dissemination of cyber-security intelligence creates a superior and more productive environment where all participants, both government and non-government, more readily share sensitive information. Building trusted relationships with stakeholders becomes essential to avoiding such limited information exchange and is a fundamental ingredient to a successful response strategy. Furthermore, a non-government entity can be a single point of interaction for all government agencies, as well as other public and private entities, charged with working with partners throughout the nation and the world to collaboratively create the expertise, information, and tools that people and communities need to protect themselves.

2. Senator Lieberman's cybersecurity bill, S. 2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Please explain your response.

While transparency is always helpful, especially when the performance requirement is to demonstrate that CI owners are at least considering and prioritizing their cybersecurity issues, there is much we don't know about the efficacy of requiring specific performance requirements. To efficiently fight the cyber threat we need realistic outcome based solutions, enabled by a data driven approach to research, development, policies and regulations. There is an emerging science of cyber security, and I encourage the Subcommittee to support practices that are both scientifically and operationally validated as part of a continuing dialogue on important policy discussions. Given the preponderance of threats, standards, technologies, products, best practices, etc. in cyber security, I strongly encourage you to emphasize the need for *operationally and scientifically sound capabilities*. Not every best practice scales well, and not every technology has scientifically sound evidence of its efficacy *and* its limitations. The academic research community increasingly recognizes the need for such sound methods as evidenced by the recent report: Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program[1] which highlights the need for "Developing a strong, rigorous scientific foundation to cybersecurity."

More research is critical to understanding requirements and solutions that will function as intended. However, currently researchers have limited access to data, resulting in sub-par solutions and stifling innovation. To truly begin to combat the cyber threat we must gain better awareness of threat indicators, and it is the federal government's role to engender access to such data beyond what any private entity has the incentive to produce. Richer data needs to be shared with the research community, not only incident data itself, but also data-sets that will enable an understanding of what "normal" resembles, enabling the detection of malicious markers that are invariant, such as behavioral based indicators (e.g. insider threats). Presently, there is not a clear understanding of what this data set would look like; but if situational awareness is to develop beyond simple indicators, the research comminute needs access to everyday data, so that we can begin to recognize what data sets are important.

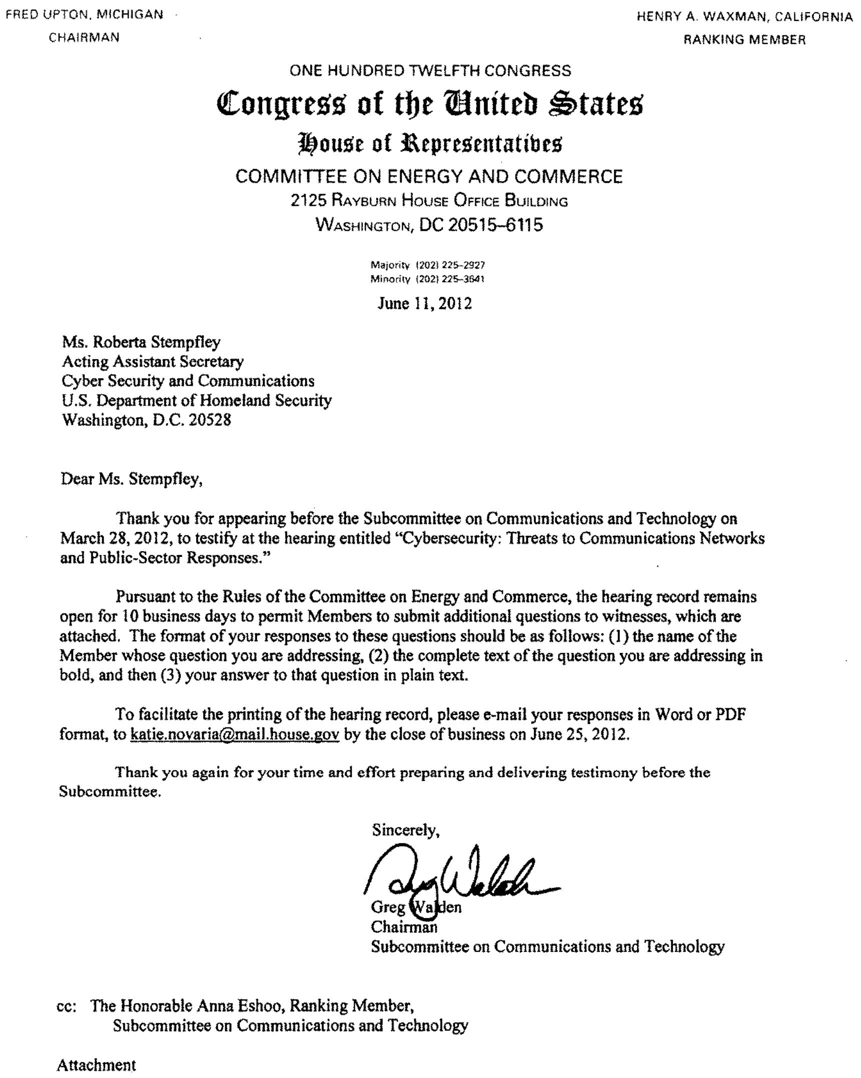
3. Similarly, do you believe the promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber-threats? Please explain your response.

There is clearly potential for un-validated performance requirements to stifle innovation since they might have unintended consequences. While, security and innovation have an uneasy relationship – both are required for our nation's security and prosperity, especially with the Internet and digital capabilities providing a unique global frontier. Again, there is a need for research and pilot studies to ensure the efficacy of regulation without impacts on performance or the suffocation of innovation.

4. Can and should CSRIC's recommendations be adopted by the FCC or other federal agencies and thereby be made mandatory? Please explain your response.

We would encourage further adoption, but advocate additional review and validation before designating them as mandatory.

[1] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf



FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 Rayburn House Office Building
Washington, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

June 11, 2012

Ms. Roberta Stempfley
Acting Assistant Secretary
Cyber Security and Communications
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Stempfley,

Thank you for appearing before the Subcommittee on Communications and Technology on March 28, 2012, to testify at the hearing entitled "Cybersecurity: Threats to Communications Networks and Public-Sector Responses."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for 10 business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and then (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please e-mail your responses in Word or PDF format, to katie.novaria@mail.house.gov by the close of business on June 25, 2012.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: The Honorable Anna Eshoo, Ranking Member,
Subcommittee on Communications and Technology

Attachment

Question#:	1
Topic:	consumer awareness
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable Anna Eshoo
Committee:	ENERGY & COMMERCE (HOUSE)

Question: I applaud your online cybersecurity consumer awareness efforts. Have you found that consumer awareness programs like "Stop, Think, and Connect" have been effective in reducing consumer vulnerability to cyber threats?

Response: In 2009, President Obama recognized the need to increase the national dialogue about cybersecurity in his Cyberspace Policy Review. As part of this review, the Department of Homeland Security (DHS) was asked to create an ongoing cybersecurity awareness campaign to help Americans understand the risks that come with being online. In conjunction with National Cyber Security Awareness Month, the Department has developed the *Stop.Think.Connect.*™ to increase public understanding of cyber threats and empower Americans to be safer and more secure online.

With its multiple facets, the campaign engages Federal, state, and local entities; industry; academia; nonprofits; and individual citizens in an ongoing dialogue on the impact Internet safety has on all segments of the community. By providing cybersecurity tools and resources to stakeholders, the Department hopes the campaign, which reaches millions of Americans through its partnerships and activities, will arm them with knowledge and actionable steps to be safer online. To spread cybersecurity awareness across the country to people of all ages and to expand the reach of *Stop.Think.Connect.*™, the Campaign established the National Network, which is a coalition comprised of non-profit organizations that advocate and promote cybersecurity internally and to their external stakeholders. Since 2011, several national organizations have joined the National Network, including Drug Abuse Resistance Education (D.A.R.E.), Boys and Girls Clubs of America, Young Women's Christian Association, 4-H, the North-American Interfraternity Council, the Advanced Cyber Security Center, and Girl Scouts of the USA. The Campaign is also in advanced discussions about National Network membership with Neighborhood Watch, the National Sheriffs Association, the National Crime Prevention Council, the Association of American Educators, and the National PanHellenic Conference. In 2010, the Campaign also launched its Cyber Awareness Coalition, which serves as an outlet for Federal agencies and state and local governments to work directly with DHS to promote awareness about cyber threats within their organizations and to the general public. Through its National Network and Cyber Awareness Coalition members, the *Stop.Think.Connect.*™. Campaign is reaching a large cross section of the American public and increasing awareness of cybersecurity risks and safe online practices.

Question#:	1
Topic:	consumer awareness
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable Anna Eshoo
Committee:	ENERGY & COMMERCE (HOUSE)

While it is difficult to quantify the reduction in consumer vulnerability, the Department is exploring methods for measuring increased national awareness as the *Stop.Think.Connect.*™ campaign enters its second full year. The difficulties in measurement currently stem from a variety of factors, including the multiple components involved in calculating vulnerability, the difficulty in measuring the degree of threats, variables associated with both threat and vulnerability (e.g. a reduction in the number of malware-infected computers could be attributed to a wide variety of causes), and the difficulties in collecting and analyzing data. As such, definitive measurements of reduction of consumer vulnerability are not currently available.

Question#:	2
Topic:	training
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable Anna Eshoo
Committee:	ENERGY & COMMERCE (HOUSE)

Question: How widely used is the DHS/FEMA Certified Cyber Security Training that you've made available online?

Response: The Federal Emergency Management Agency's (FEMA) National Training and Education Division (NTED) offers 10 on-line courses on Cyber Security through Texas Engineering Extension Service (TEEX), a member of the National Domestic Preparedness Consortium (NDPC). This DHS/FEMA Certified Cyber Security Training is designed to ensure that the privacy, reliability, and integrity of the information systems that power the global economy remain intact and secure. The 10 courses are offered through three discipline-specific tracks targeting everyday non-technical computer users, technical IT professionals, and business managers and professionals.

These courses are offered at no cost and students earn a DHS/FEMA Certificate of completion along with Continuing Education Units (CEU) at the completion of each course.

The suite of courses includes the following:

Name		**Student Attendance FY**
10/11		
AWR-138-W	Network Assurance	244
AWR-139-W	Digital Forensics Basics	213
AWR-168-W	Cyber Law and White Collar Crime	146
AWR-169-W	Cyber Incident Analysis and Report	109
AWR-173-W	Information Security Basics	615
AWR-174-W	Cyber Ethics	312
AWR-175-W	Information Security for Everyone	1684
AWR-176-W	Business Information Continuity	225
AWR-177-W	Information Risk Management	123
AWR-178-W	Secure Software	330

Question#:	2
Topic:	training
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable Anna Eshoo
Committee:	ENERGY & COMMERCE (HOUSE)

NTED also offers 3 Cyber Security courses through Norwich University Applied Research Institutes (NUARI).

These courses include the following:

AWR-222-W	Cyber Incident Awareness Training, Web-Based	New Course
AWR-223-W	Emergency Management for IT Professionals, Web-Based	New Course
AWR-299-W	Cyber Exercise Participant Training, Web-Based	New Course

Question#:	3
Topic:	information sharing
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable John D. Dingell
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Industry witnesses told this Subcommittee on March 7, 2012, that the federal government should facilitate better intra-industry and public-private information sharing. Do you agree with that opinion? Please explain your response.

Response: The Department of Homeland Security (DHS) encourages intra-industry information sharing largely through its convening power. Numerous discussions and interactions with industry partners have shown that the most productive role for the Federal Government would be to allow intra-industry information sharing relationships to develop and sustain themselves with little to no government intervention.

The Federal Government, with DHS as the lead, has a vital role to play as the facilitator of public-private information sharing and will continue to improve upon current efforts. Cybersecurity for critical infrastructure operates most effectively when there is close operational collaboration and information sharing between the public and private sectors. Government and industry each possess valuable information that the other party may not have. This information, when shared appropriately and in a secure environment, can contribute to the overall cybersecurity of the parties and the entire Nation.

The foundation for private-sector engagement is the sector partnership framework established under the National Infrastructure Protection Plan (NIPP). The NIPP enables and encourages DHS to work closely with public- and private-sector critical infrastructure through a series of sector and cross-sector councils that span the 18 critical infrastructure sectors, as well as with individual owners and operators.

Both private and public sector entities should understand that some barriers to information sharing serve a valuable purpose, and developing the information sharing process is – and will remain – an ongoing task that involves the balancing of complex, sometimes competing equities. Private entities are often fearful that sharing information with the government will result in widespread dissemination of corporate information that may cause commercial harms or jeopardize the rights and interests of their employees, investors and clients. In response to that concern, DHS relies on the Protected Critical Infrastructure Information (PCII) scheme, which allows those who report to the Government to do so in confidentiality, to ensure the protection of sensitive or proprietary information, including information that could damage the rights or interests of employees, clients or shareholders. This necessarily limits DHS information sharing, but it protects the rights of private sector sources and encourages them to report cyber incident information. DHS always seeks to maximize the dissemination of cyber threat

Question#:	3
Topic:	information sharing
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable John D. Dingell
Committee:	ENERGY & COMMERCE (HOUSE)

information but respects PCII and other privacy and civil liberties limitations by anonymizing threat information, redacting personal identifying information if feasible, and by maintaining confidentiality where information cannot be shared outside of Government channels without jeopardizing the private sector source's interests.

At the same time, some of the barriers to the sharing of government-derived threat information are similar to PCII constraints, and exist to protect the rights of victims and innocent third parties, and to protect the operational integrity of government cybersecurity activities. The end result of balancing these interests, in many cases, is a widely disseminated, unclassified threat awareness document that identifies a particular threat and methods for dealing with it. To the extent possible, the threat awareness document will contain little or no personal identifying information, no sensitive or proprietary information, and no information that would tend to compromise government cybersecurity efforts. The absence of these elements of information is often unsatisfying to the consumers of reports, but it is the result of protecting the rights of those affected by the cybersecurity incident that is the subject of the report.

Access to all potential threat information across the public and private sectors is not absolute, and must balance the protection of the rights of the individuals and institutions affected by cyber incidents, and maintain the operational integrity of our cybersecurity efforts. DHS believes that it is currently doing a good job of balancing these competing equities, but realizes that diligent, continuous efforts are necessary to ensure ongoing improvement in private/public cybersecurity information sharing.

The Department supports legislation that would further these efforts. DHS understands that Senator Lieberman recently introduced a new version of the Cybersecurity Act of 2012. The Administration is currently reviewing this version of the bill and looks forward to working with the Congress as the bill moves through the legislative process.

Question#:	4
Topic:	cybersecurity bill
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable John D. Dingell
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Senator Lieberman's cybersecurity bill, S. 2105, requires the Secretary of Homeland Security to promulgate risk-based cybersecurity performance requirements for owners of critical infrastructure. Do you believe the promulgation of such requirements is wise? Please explain your response.

Response: Risk-based cybersecurity best practices—developed in consultation with the Federal interagency, state and local government, and the private sector—would enhance the cybersecurity of our Nation's critical infrastructure.

Cybersecurity best practices would focus on outcomes rather than specific technical controls. Covered critical infrastructure owners, therefore, would have the freedom to select and implement the cybersecurity measures that they determine best satisfy the requirements. While cybersecurity best practices thus would help establish a baseline of cybersecurity performance for critical infrastructure, they would not dictate that owners adopt any specific technical control or other risk mitigation action.

Question#:	5
Topic:	cyber-threats
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable John D. Dingell
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Similarly, do you believe the promulgation of such performance requirements would stifle innovation and harm industry's ability to protect consumers from cyber-threats? Please explain your response.

Response: Cybersecurity best practices, as opposed to technical controls, are inherently flexible. Best practices would establish a baseline of cybersecurity performance for critical infrastructure, but they would not dictate that owners adopt any specific technical control or other risk mitigation action. The focus on outcomes, therefore, may promote innovation by encouraging the private sector to develop new cybersecurity offerings at affordable cost to address the needs of critical infrastructure owners. As a result, consumers would be better protected from cyber threats.

Question#:	6
Topic:	CSRIC's
Hearing:	Cybersecurity: Threats to Communications Networks and Public-Sector Responses
Primary:	The Honorable John D. Dingell
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Can and should CSRIC's recommendations be adopted by the FCC or other federal agencies and thereby be made mandatory? Please explain your response.

Response: The Department of Homeland Security strongly supports the Federal Communications Commission's and other Federal agencies' continued, serious consideration of the Communications Security, Reliability, and Interoperability Council (CSRIC) recommendations and how to integrate them into appropriate voluntary, regulatory, and government-procurement regimes. However, CSRIC is a dynamic mechanism, where providers are actively engaged and frequently make voluntary commitments to comply with resulting recommendations. While these recommendations are very valuable, they are not currently written in a way that allows for them to be easily or expeditiously adopted as mandatory requirements, which would require conducting a rulemaking proceeding.