AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

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 7, 2012

Serial No. 112–123

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
77–040 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
JAY INSLEE, Washington
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

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)*

C O N T E N T S

	Page
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	1
Prepared statement	4
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	6
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	6
Hon. Doris O. Matsui, a Representative in Congress from the State of California, opening statement	7
Hon. Lee Terry, a Representative in Congress from the State of Nebraska, opening statement	8
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	8
Hon. Henry A. Waxman, a Representative in Congress from the State of California, opening statement	9
Prepared statement	11
WITNESSES	
Jason Livingood, Vice President, Internet Systems Engineering, Comcast Corporation	13
Prepared statement	15
Answers to submitted questions	102
Edward Amoroso, Chief Security Officer, AT&T Services, Inc.	34
Prepared statement	36
Answers to submitted questions	106
David Mahon, Chief Security Officer, CenturyLink	48
Prepared statement	50
Answers to submitted questions	110
John Olsen, Senior Vice President and Chief Information Officer, MetroPCS Communications, Inc.	56
Prepared statement	58
Answers to submitted questions	114
Scott Totzke, Senior Vice President, BlackBerry Security Group, Research in Motion	67
Prepared statement	69
Answers to submitted questions	118

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

WEDNESDAY, MARCH 7, 2012

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

The subcommittee met, pursuant to call, at 10:04 a.m., in room 2123 of the Rayburn House Office Building, Hon. Greg Walden (chairman of the subcommittee) presiding.

Members present: Representatives Walden, Terry, Stearns, Shimkus, Bono Mack, Rogers, Blackburn, Bilbray, Bass, Gingrey, Scalise, Latta, Guthrie, Kinzinger, Eshoo, Doyle, Matsui, Barrow, Christensen, DeGette, Dingell, and Waxman (ex officio).

Staff present: Ray Baum, Senior Policy Advisor/Director of Coalitions; Nicholas Degani, FCC Detailee; Neil Fried, Chief Counsel, Communications and Technology; Debbee Keller, Press Secretary; Katie Novaria, Legislative Clerk; Andrew Powaleny, Deputy Press Secretary; David Redl, Counsel, Communications and Technology; Roger Sherman, Democratic Chief Counsel, Communications and Technology; Jeff Cohen, FCC Detailee; Shawn Chang, Democratic Senior Counsel, Communications and Technology; Hadass Kogan, Democratic Legal Fellow; and Kara Van Stralen, Democratic Special Assistant.

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

Mr. WALDEN. We will call to order the Subcommittee on Communications and Technology for a hearing on "Cybersecurity: The Pivotal Role of Communications Networks." I want to thank our witnesses for being here this morning. We look forward to your testimony and are very appreciative of your taking the time to be here to help educate us so we can do the right thing in terms of assisting you all, particularly the security networks or the cyber networks.

Back in October, the House Republican Cybersecurity Task Force appointed by the Speaker recommended that the committees of jurisdiction review cybersecurity issues. This subcommittee has embarked on a series of hearings to heed that call and to get a complete picture of the cybersecurity challenges that our Nation faces.

In our February 8 hearing, we examined threats to communications networks and the concerns of the private sector security firms helping to secure those communications networks. That hearing

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 steps that network operators have taken to secure their networks and any recommendations that you all might have on how Congress can help, actually help in those efforts.

As we heard in the February 8 hearing, threats to communications networks have come a long way in a very short period of time. Before coming to Congress, I spent 22 years as a radio broadcaster, and as a small businessperson, I had to worry about securing our own communications network, but those were simpler times. In modern communications networks of all types, cybersecurity has become a pressing concern. In our February 8 hearing, we had a dizzying array of new cybersecurity threats discussed like supply chain vulnerabilities, botnets, and Domain Name System spoofing.

On the brighter side, we were also told during that hearing about several potential solutions to make communications networks more secure. This is why I have asked a number of my colleagues to serve as the Communications and Technology Cybersecurity Working Group. The working group is a bipartisan team of six subcommittee members, led by Subcommittee Vice Chair Lee Terry and Subcommittee Ranking Member Anna Eshoo, that will look into some of these potential solutions and the legal and regulatory impediments to securing communications networks against cyber threats. With an eye toward incentive-based approaches, the working group looks to facilitate communication among private sector companies and the public sector on a variety of topics, including DNSSEC adoption, supply chain risk management, and a voluntary code of conduct and best practices for network operators.

Now, in this hearing, we are privileged to have five witnesses that represent parts of the commercial network to guide us through the complex cybersecurity issues that you each face. Network operators own, maintain and operate most of the infrastructure that makes up our communications networks. Their management of the wires, the towers, the base stations, the servers and the wireless handsets that are integral parts of communications networks put these companies on the front lines of cybersecurity. I want to know what cybersecurity services and educational initiatives are being aimed at your consumers, what steps are being taken to secure the core components that make up our communications networks, and what affirmative steps network operators have taken to secure the supply chain and to prevent cyber attacks.

I would also expect to hear what you think the appropriate role of the Federal Government is to combat cyber threats. Are Federal laws and regulations helping or hindering information sharing? Are there cybersecurity solutions that your company has identified that would prevent cyber attacks, but would run afoul of existing laws? How can the Federal Government incent network operators and other members of the private sector to invest and innovate in the cybersecurity arena? And coming off of our prior hearing on February 8, how do we make sure that we don't put things in statute that cause misallocation of your capital and make you less nimble

in this extraordinary cyber threat environment. So I look forward to your testimony today.

[The prepared statement of Mr. Walden follows:]

Statement of the Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
Hearing on "Cybersecurity: The Pivotal Role of Communications Networks"
March 7, 2012

(As Prepared for Delivery)

Back in October, the *House Republican Cybersecurity Task Force* recommended that the committees of jurisdiction review cybersecurity issues. This subcommittee has embarked on a series of hearings to heed that call and to get a complete picture of the cybersecurity challenges our nation faces. In our February 8 hearing, we examined threats to communications networks and the concerns of the private sector security firms helping to secure communications networks. That hearing 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 steps that network operators have taken to secure their networks and any recommendations they may have on how Congress can help in those efforts.

As we heard in the February 8 hearing, threats to communications networks have come a long way in a short time. Before coming to Congress, I spent 22 years as a radio broadcaster. As a small businessman, I had to worry about securing our communications network, but those were simpler times. In modern communications networks of all types, cybersecurity has become a pressing concern. In the February 8 hearing, we heard about the dizzying array of new cybersecurity threats, like supply chain vulnerabilities, botnets and Domain Name System spoofing.

On the brighter side, we were also told during that hearing about several potential solutions to make communications networks more secure. This is why I have asked a number of my colleagues to serve on the Communications and Technology Cybersecurity Working Group. The working group is a bipartisan team of six subcommittee members – led by Subcommittee Vice-Chairman Lee Terry and Subcommittee Ranking Member Anna Eshoo – that will look into some of these potential solutions and the legal and regulatory impediments to securing communications networks against cyberthreats. With an eye toward incentive-based approaches, the working group looks to facilitate communication among private sector companies and with the public sector on a variety of topics, including DNSSEC adoption, supply chain risk management, and a voluntary code of conduct and best practices for network operators.

In this hearing, we are privileged to have five witnesses that represent parts of the commercial network to guide us through the complex cybersecurity issues that they face. Network operators own, maintain, and operate most of the infrastructure that make up our communications networks. Their management of the wires, the towers, the base stations, the servers, and the wireless handsets that are integral parts of communications networks put these companies on the front lines of cybersecurity. I want to know what cybersecurity services and educational initiatives are being aimed at consumers, what steps are being taken to secure the

core components that make up our communications networks, and what affirmative steps network operators have taken to secure the supply chain and to prevent cyberattacks.

I also expect to hear what you think the appropriate role of the federal government is to combat cyberthreats. Are federal laws and regulations helping or hindering information sharing? Are there cybersecurity solutions that your company has identified that would prevent cyberattacks, but would run afoul of existing laws? How can the federal government incent network operators and other members of the private sector to invest and innovate in the cybersecurity arena?

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

Mr. WALDEN. I would yield time to Ms. Blackburn.

Mrs. BLACKBURN. Thank you, Mr. Chairman. Welcome to all of you, and we are deeply appreciative of your time for being here.

I think one of the things that——

Mr. WALDEN. Could you get a little closer to your microphone?

Mrs. BLACKBURN. I certainly can. I am a mother. I can always talk louder. That is right.

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

The GAO report that mentioned we have seen a 650 percent growth in cyber attacks over the past 5 years, I think that that caused a lot of people to, you know, sit up and take note of what might be happening out there, because you look at the attacks, you look at what that equates to an effect on the economy. Chairman Bono Mack and I are working on introducing a bill, the cybersecurity bill here in the House, similar to secure IT from the Senate, and I think the concepts we are viewing are not to be overly prescriptive and to kind of work off the first principle of "do no harm" and have a good, broad conversation in this. I would love to hear you all talk a little bit about government networks and the importance you think and responsibility you think government has in securing its own networks and system. I would love to also hear a little bit from you about incentive-based security and how we approach that.

With that, I yield back.

Mr. WALDEN. I thank the gentlelady for her comments and now recognize my friend from California, 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 welcome to all of the witnesses and thank you for being here today.

As the title of today's hearing suggests, our communications networks are part of the backbone of our Nation's critical infrastructure. From electricity generation to financial service and transportation, we depend on our communications networks for nearly all aspects of our daily lives. Yet as was highlighted during our first cybersecurity hearing, our networks remain vulnerable to attack.

In particular, there are three areas I would like to hear more about from our witnesses today. First, as we discussed in last month's hearing, the FCC chairman is currently proposing a voluntary ISP code of conduct as a way to alert consumers when a botnet or other malware infection is discovered. So today's witnesses will be on the front line in ensuring such best practices are effectively implemented and obviously I think that you are going to talk about that, and I look forward to it.

Second, I would like to hear more about your views on the supply chain security. I continue to have really grave concerns stemming from my 8 years that I just recently completed at the House Intelligence Committee about the implications of foreign-controlled tele-

communications infrastructure companies providing equipment to the U.S. market. In 2010, I wrote to the FCC chairman asking for a better understanding of the FCC's authority to address these challenges and what kind of transparency requirements should be placed on companies seeking to sell telecommunications infrastructure equipment to U.S. network providers.

Third, I would like to learn more about any unique challenges in securing mobile networks. As more data is transmitted wirelessly, we need to look closely at how these networks are secured to ensure they don't become the entryway to the broader network.

So today's hearing is an important aspect of our subcommittee's work on cybersecurity. Again, I want to thank each one of our witnesses for being willing to testify today to be instructive to us, and I want to thank the chairman for the spirit of cooperation around this issue. Usually there are some Democratic witnesses that are called and Republican witnesses. That is not the case today. So this is something that rises above that, and I look forward to working with the entire committee so that we not only better understand the cybersecurity challenges facing communications networks but what steps we can take to secure them and thereby strengthen the country.

I would like to yield my remaining time to Representative Matsui.

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

Ms. MATSUI. Thank you, Ranking Member Eshoo, for yielding me time. Mr. Chairman, thank you for holding today's hearing, and I want to thank the witnesses for being here today.

There is no doubt that cyber attacks are real and continue to pose significant threats to several aspects of our economy, and Mr. Chairman, I am pleased that you and Ranking Member Eshoo formed a bipartisan cyber working group so that we can appropriately explore our subcommittee's interest to enhance our Nation's efforts against a cyber attack.

There are a variety of issues that we may explore. Communications networks are one of the many areas that our Nation must protect and ensure safety and soundness. Advancing IP-based technologies and public safety communications heighten the concerns for cybersecurity. It would be important that data is protected from a PC or a cell phone in transit to cloud storage, particularly as more and more Americans send personal information to the cloud.

I also believe that our subcommittee will have the ability to further promote information sharing on cyber threats. Securing the supply chain will be of high importance so that tech components remain secure through their manufacturing and distribution processes. Among others, I believe that R&D incentives could encourage industry to explore ways to better address and defend against malware and botnets.

Again, I thank the chairman for holding today's hearing. I look forward to working with my colleagues on ways that this subcommittee can encourage greater protection against cyber threats. I thank the witnesses for appearing today.

I yield back the remainder of my time.

Mr. WALDEN. I thank the gentlelady for her comments.

I will now recognize the vice chairman of the committee, Mr. Terry, for opening comments.

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

Mr. TERRY. Thank you, Chairman, and let me start by saying that I believe that most of my colleagues on this committee share my optimism that a collaborative, active cyber defense capability is actually achievable. There might be a few differences in opinion on what needs to be done to reach this goal, but through the bipartisan conversations like those taking place in the working group and public hearings like this, we are getting closer.

In reading through the written testimony provided by today's witnesses, I noticed a common threat throughout. As Mr. Amoroso eloquently says, "Quite simply, innovation is inconsistent with standardization." I agree wholeheartedly with our witness, and in my opinion, I find this to be the most vital guiding principle in considering how to enhance our Nation's cybersecurity. In fact, as I continue to dig deeper on this issue, I become more convinced that any sort of legislative effort to provide overbroad regulation or certification regimes will surely come with unintended consequences. Instead, ISPs should have the flexibility to respond to real-time security threats in a manner that minimizes delay and maximizes their ability to innovate as they strive to protect their consumers and their network.

A couple of things I believe that we can do to help reach the goal of collaborative active cyber defense capability are, one, remove the current barriers in place that prevention communication networks from sharing cyber threat information with the government agencies and also with the private sector entities. Provide adequate liability protection in order for the sharing of cyber threat information is second.

Again, I thank our witnesses for joining us today, and shall I yield to Mr. Stearns.

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

Mr. STEARNS. I thank my colleague.

My colleagues, I think the consistent message from our witnesses today is that the private sector has very strong commercial incentives to invest in and maintain robust cybersecurity. In fact, each of our witnesses today has described unique and thorough approaches to protecting their own networks. These examples demonstrate that one-size-fits-all legislation is not the appropriate solution to cybersecurity threats. Moreover, because these threats change every day, industry must be provided the flexibility to respond quickly to an attack.

Therefore, I believe that prescriptive top-down government mandates are not only unnecessary but they simply will not work. Instead, government should seek to improve information sharing and consumer education. We also should work to eliminate outdated

regulations that have created unintentional barriers toward ensuring the security of our networks.

So I look forward to our witnesses today and I thank you, Mr. Chairman, for this great hearing.

Mr. WALDEN. Are there any other member seeking time on our side? If not, the gentleman yields back his time and I recognized the gentleman from California, Mr. Waxman, for an opening statement.

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

Mr. WAXMAN. Thank you very much, Mr. Chairman, and I welcome our witnesses as well.

I am pleased that that the subcommittee is looking at this issue of cybersecurity. This is our second hearing. Every week we learn of a new cyber breach or vulnerability, so it is vital that we are paying attention to this question.

Like the smart grid, which was the topic of our last hearing by the subcommittee on Oversight and Investigations, communications networks are highly vulnerable to cyber attack. The potential for severe disruptions are high because communications networks are the common thread to all critical infrastructure sectors.

In fact, the public safety legislation that was just signed into law exemplifies these concerns. Under the new law, first responders will be relying on broadband communications networks to secure the safety of life and property. That will strengthen their ability to protect the public, but only if the networks are protected from cyber attacks.

Today, I look forward to continuing our discussion of the security threats faced by mobile devices and the proper role for this subcommittee in ensuring cybersecurity. Our witnesses today represent a broad cross-section of Internet service providers, as well as a handset manufacturer. This should further help our understanding of what risks threaten communications networks, what companies are doing to mitigate these risks, and what the subcommittee might do to assist you in these efforts.

I believe the Federal Government has an important role to play in ensuring the cybersecurity of the Nation's communications networks. One important Federal role is developing practices that will keep the Internet safe. The FCC's upcoming release of its cyber best practices report, developed by the well-regarded Communications Security, Reliability and Interoperability Council, such a long name that is reduced to CSRIC, will provide valuable guidance to industry and our subcommittee.

I understand the chairman is planning a third hearing with government agencies. I commend him for this series of hearings and look forward to what our witnesses have to tell us.

And finally, I want to join in thanking you, Mr. Chairman, for organizing a bipartisan working group to study cyber threats and inform the subcommittee of its findings. This is a good opportunity for subcommittee members and staff to work together on an issue of common concern. I look forward to hearing back from the work-

ing group and exploring with the subcommittee potential further actions.

Thank you for the hearing. I thank all the witnesses for being here. I look forward to the testimony. Yield back.

[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: The Pivotal Role of Communications Networks"
Subcommittee on Communications and Technology
March 7, 2012

I am pleased that that the Subcommittee is holding this second hearing on cybersecurity. Nearly every week we learn of a new cyber breach or vulnerability, so it is vital that the Communications Subcommittee is focusing on this topic.

Like the smart grid, which was the topic of a hearing by the Subcommittee on Oversight and Investigations last month, communications networks are highly vulnerable to cyber attack. The potential for severe disruptions are high because communications networks are the common thread to all critical infrastructure sectors.

In fact, the public safety legislation that was just signed into law exemplifies these concerns. Under the new law, first responders will be relying on broadband communications networks to secure the safety of life and property. That will strengthen their ability to protect the public – but only if the networks are protected from cyber attacks.

Today, I look forward to continuing our discussion of the security threats faced by mobile devices and the proper role for this Subcommittee in ensuring cybersecurity. Our witnesses today -- representing a broad cross-section of internet service providers, as well as a handset manufacturer -- should further help our understanding of what risks threaten communications networks, what companies are doing to mitigate these risks, and what the Subcommittee might do to assist these efforts.

I believe the federal government has an important role to play in ensuring the cybersecurity of the nation's communications networks. One important federal role is developing practices that will keep the internet safe. The FCC's upcoming release of its cyber best practices report – developed by the well-regarded Communications Security, Reliability and Interoperability Council or "CSRIC" – will provide valuable guidance to industry and the Subcommittee.

I understand Chairman Walden is planning a third hearing with government agencies. I commend him for this series of hearing and look forward to hearing from witnesses representing the FCC and other relevant agencies.

Finally, I want to thank Chairman Walden for organizing a bipartisan working group to study cyber threats and inform the Subcommittee of its findings. This is a good opportunity for Subcommittee members and staff to work together on an issue of common concern. I look forward to hearing back from the working group and exploring with the Subcommittee potential further actions.

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

Mr. WALDEN. The gentleman yields back his time. I thank you for your comments. We have a lot of big brains on this committee and we are going to need them all to protect America, so thank you to the members who have agreed to serve on that working group.

Gentlemen, we are delighted to have you here today. We will start with Mr. Livingood. We appreciate your being here, Vice President, Internet Systems Engineering from Comcast Corporation. Thank you for being here. Just a friendly reminder, being an old radio guy: Pull these microphones very close and make sure the button is lit and you will be good to go.

STATEMENTS OF JASON LIVINGOOD, VICE PRESIDENT, INTERNET SYSTEMS ENGINEERING, COMCAST CORPORATION; EDWARD AMOROSO, CHIEF SECURITY OFFICER, AT&T SERVICES, INC.; DAVID MAHON, CHIEF SECURITY OFFICER, CENTURYLINK; JOHN OLSEN, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, METROPCS COMMUNICATIONS, INC.; AND SCOTT TOTZKE, SENIOR VICE PRESIDENT, BLACKBERRY SECURITY GROUP, RESEARCH IN MOTION

STATEMENT OF JASON LIVINGOOD

Mr. LIVINGOOD. OK. Thank you very much, Mr. Chairman, Ranking Member Eshoo and members of the subcommittee for inviting me to discuss some of the work that Comcast is doing to protect consumers and cyberspace. We appreciate the subcommittee's interest in this issue and its willingness to hear the perspective of someone like me, an engineer working in cybersecurity and other technical Internet issues every day.

I serve as Vice President of Internet Systems Engineering at Comcast, and I am the Engineering Leader in charge of our residential high-speed Internet service. I currently serve on an FCC CSRIC working group, on ICANN's Security and Stability Advisory Committee, on the Broadband Internet Technical Advisory Group, and am a member of the board of trustees of the Internet Society. I am also an active contributor of the Internet Engineering Task Force, or IETF.

At Comcast, we take cybersecurity issues seriously, and we know that our customers are very concerned about security. We strive to provide them with the best, fastest and most secure Internet service possible, and our engineering team devotes significant time, energy and investment to constantly update and refine our cybersecurity efforts.

One such threat that we focused on comes from malicious software called a bot. Bots run on an end user's computer without their knowledge and are controlled remotely. Bots are used to conduct identity and credit card theft, denial of service attacks, steal user names and passwords, and send spam. It is important to understand that a person need not consciously do something like download an app to become infected. Sometimes they can be infected just by visiting a Web site.

To counter bots, we developed a system called Constant Guard. This customer-facing system first detects botnet traffic, notifies end users of infection such as sending them alerts in their web browser, and provides them with tools to remove those infections.

Another area of threat is to the Domain Name System, which is a foundational and extraordinarily important and critical part of the Internet. The Domain Name System, or DNS for short, is responsible for basically translating names like Comcast.com into IP addresses, which are the addresses used to connect and route traffic across the Internet. So it is extremely important. But a vulnerability in the DNS can permit an attacker to inject a fake answer into the DNS. An attacker, for example, can then direct traffic destined to a site such as a banking Web site to computers that they control, perhaps to collect login and financial information, but the address in the user's web browser still appears correct.

The long-term fix is to implement DNS security extensions, or DNSSEC for short. This involves someone doing two things. First, cryptographically signing the domain names that they own and then Internet service providers validating those signatures before connecting a user to that site. This is basically akin to your bank keeping your signature on file and checking the signature on your check against that before cashing your check.

It is important to note that DNSSEC was developed via an international multi-stakeholder process at the IETF and will require adoption across the entire ecosystem such as by banks, web browsers, software companies and cloud services, not just ISPs. I am pleased to report as part of Constant Guard, Comcast was the first ISP in the United States to fully deploy DNSSEC in January.

But it is important to understand that no open and massively interconnected network can ever be completely and totally secure. While there is no perfect solution to security, that does not mean that there are no good solutions, so our focus has been quite simply to roll up our sleeves and get to work chipping away at the security threats day in and day out, quickly learning and adapting. We are working within the industry and on a global basis to combat the key threats and to protect our customers the best that we can and also to help them protect themselves. There are powerful incentives to take strong and effective measures to ensure network security and safety. Our consumers want assurance that the networks that they are using are safe and secure, and we have strong reasons therefore to invest capital and resources into cybersecurity safeguards. The same is of course true for other network providers. We all have powerful incentives to take actions necessary to secure our substantial investments in our networks.

Policymakers can help these efforts by removing legal uncertainties that can inhibit collaboration while preserving and strengthening this flexibility that providers have to develop the best solutions for each of our networks. As one of the members said a moment ago, there is no one-size-fits-all solution, so flexibility is key, and it is important because the threats change as rapidly as they do. Flexibility will help to ensure that we can continue to focus on security and innovation rather than compliance and regulation.

Thank you.

[The prepared statement of Mr. Livingood follows:]

TESTIMONY OF JASON LIVINGOOD
VICE PRESIDENT, INTERNET SYSTEMS ENGINEERING
COMCAST CORPORATION

on

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

before the

Committee on Energy and Commerce
Subcommittee on Communications and Technology

UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

MARCH 7, 2012

TESTIMONY OF JASON LIVINGOOD
VICE PRESIDENT, INTERNET SYSTEMS ENGINEERING
COMCAST CORPORATION

Good morning, Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee. My name is Jason Livingood and I am the Vice President of Internet Systems Engineering at Comcast Corporation. I would like to thank you for inviting me to testify here today. Your staff asked that we share our experience with our customer-facing Internet security efforts, particularly our Constant Guard cybersecurity measures, including botnet detection, notification, and remediation mechanisms, as well as our recent deployment of Domain Name System Security Extensions (DNSSEC).

At Comcast, we take cybersecurity issues very seriously, and know that our Xfinity Internet customers are concerned about security. We strive to provide our customers with the best, fastest, and most secure Internet service we can, and our engineering team devotes significant time, energy, and investment to update and refine constantly our cybersecurity efforts.

I think we can all agree that the benefits of an interconnected world far outweigh the risks and that it is probably unrealistic to expect complete and total security in any network, including the super-fast, interconnected networks operating today. Network operators and other entities in the Internet ecosystem, however, have the important job of managing these ever-changing risks. Our experience has taught us *that there is no "one size fits all" model for addressing cybersecurity risks*. The flexibility afforded to us to design and develop the best possible security solutions that are optimally adapted to our particular network architecture and customer environment is – and must remain – a core element of any successful cybersecurity policy

framework. Attempting to impose uniform cybersecurity solutions could actually be counterproductive, by enabling an attacker that cracks a single solution to compromise multiple systems, and by slowing down or constraining our ability to rapidly develop innovative cybersecurity solutions.

Comcast is the nation's largest Internet Service Provider (ISP). With over 18 million residential and business broadband customers on one of the world's largest converged Internet Protocol-based voice, video, and data network, ensuring the safety and security of the network over which they receive our services is one of our top priorities. Deterring, detecting, and responding to cybersecurity threats is therefore a fundamental requirement for our continued business success.

Cybersecurity threats such as bot networks ("botnets") are particularly insidious because they turn ordinary users into unwitting participants in global criminal enterprises. Bots are a form of malicious software that infect a computer and allow it to be remotely controlled for nefarious and criminal purposes by a malevolent party. Some security companies estimate that as many as ten to fifteen percent of American households are likely infected. A bot can cause significant harm to the individual user, an entire network, and beyond. This threat is growing and is a major source of identity and credit card theft. Bots are also used to conduct massive Distributed Denial of Service attacks, steal user names and passwords, send spam, and facilitate other malicious and criminal activity.

Because botnets are typically surreptitiously installed on common consumer devices like personal computers, a consumer-focused approach to cybersecurity is essential to protect individual consumers, the broader infrastructure of our network, other networks, and the Internet in general. This threat becomes even more challenging when we consider the growth and

proliferation of a variety of new mobile, smart phone, tablet, and other personal devices that have Internet access, which could also be vulnerable to infection. Internet users are increasingly aware of and concerned by the numerous and constantly evolving threats to their cybersecurity. As public awareness of these issues grows, so, too, does consumer demand for comprehensive security offerings that provide peace of mind as well as a more secure Internet experience.

Comcast understands that consumer-based security tools must work in conjunction with network-based measures in order to secure end users from cyber threats. We have been at the forefront of providing a consumer-oriented security product suite aimed at preventing – and, where necessary, remediating – disruptions and damage caused by malware, viruses, bots, and other cyber threats that affect the safety and security of both our network and the customer devices connected to our network. We have invested substantial resources to provide consumer education, established a dedicated customer security assistance team, and deployed state-of-the-art technologies and applications in our networks to combat bots and other Internet threats.

With that introduction, let me first describe Comcast's general approach to cybersecurity, and then describe our efforts to combat botnets and our DNSSEC deployment.

Comcast's Approach to Cybersecurity

"Security" encompasses a broad spectrum of techniques, tools, protocols, and practices. There is no one silver bullet or quick fix, especially because the risks and threats change so very frequently and dramatically as new technology is developed and as bad actors in cyberspace continue to innovate. They constantly adapt to the latest counter-measures and employ new techniques and tools. As a result, our security protections will never be complete; we must continuously learn, adapt, and work to improve and develop new capabilities to meet the ever-changing threats. Indeed, there is no realistic possibility that any network will ever be

"completely" secure. But consumers' increasing desire for robust security protections and the need to protect our network provide Comcast with strong incentives to continuously invest in new and advanced security tools and offerings.

The threats that ISPs like Comcast observe appear to be primarily and overwhelmingly driven by economic motivations. There is a *sizable* underground economy that drives and profits from cybercrime, and this is the main threat facing individual Internet users today. Unfortunately, with respect to some threats, such as botnets, the pace of change and other complexities can render many of the available solutions from Internet security software developers outdated or inadequate for addressing the latest and most recent form of an infection. For example, software does not readily exist for consumer use which can reliably, 100 percent of the time, remove new forms of malware as soon as they are released, and do so quickly and easily. In such instances, the security risks and vulnerabilities faced by ISPs are not a function of insufficient resources or investment, but rather a reflection of the pace of adaptation and innovation demonstrated by cyber criminals and of the relative immaturity of malware remediation tools.

The available data on malware infections highlight the breadth and scope of the problem. For example:

- According to Symantec's Norton Cybercrime Report 2011, 54 percent of online adults across the globe have experienced viruses or malware on their computers. At least 10 percent of adults are estimated to have been victims of phishing scams.[1/]
- Microsoft's 2011 Security Intelligence Report estimated that approximately 10 million personal computers in the U.S. are infected with some type of malware every quarter.[2/]

1/ Available at http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

- Over one million web site URLs are estimated to host malware, and the number of impressions of advertising containing malware is estimated at 3 million per day.[3/]
- One security solutions provider has estimated that "the probability that an average Internet user will hit an infected page after three months of Web browsing is 95 percent."[4/]
- It is also estimated that between 10 and 15 percent of American households have a device which has been infected with a bot.

Comcast's Consumer-Facing Cybersecurity Offerings

The prevalence of botnet and malware problems reflects the fact that it is relatively easy for a device to become infected. There is a misconception among the public at large that online users cannot become infected unless they download a program or application presented to them – but that is simply not the case. A user's personal computer can become infected through such common acts as opening an email that may contain a virus, clicking on a web site that shows up in a search result but serves as a host for a virus, or even by clicking on an ad or link that launches a hidden virus while navigating a legitimate web site. It is possible for the end user's device to become infected via a so-called "drive-by infection," where someone gets infected just by visiting a web site. For example, a site may itself be secure but the advertising network it uses may show an advertisement that has an embedded malware code, and the advertisement need only be displayed rather than clicked for an infection to occur.

2/ Microsoft Security Intelligence Report, Vol. 11, June 2011, available at http://www.microsoft.com/security/sir/default.aspx

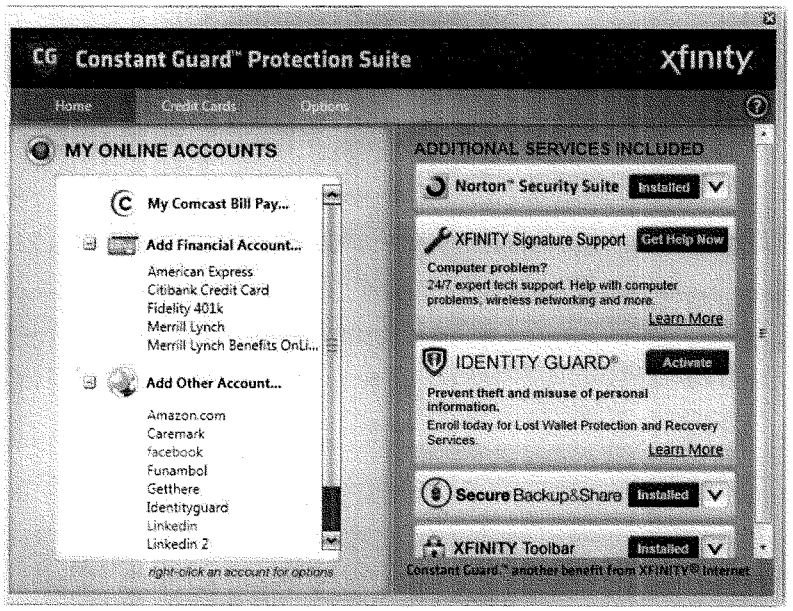
3/ "Report: malware-laden sites double from a year ago," http://news.cnet.com/8301-27080_3-20040367-245.html?tag=mantle_skin;content, March 8, 2011.

4/ *Id.*

At Comcast, we understand that securing cyberspace is a complex task that requires multiple approaches. Education, prevention, detection, remediation, and recovery are the core objectives of our anti-malware efforts, which include our comprehensive security suite, Constant Guard.

Constant Guard offers a multilayered, holistic approach to Internet security that provides protection, detection, notification, and remediation for our customers. Constant Guard combines extensive technological resources, including software such as the Norton Security Suite, anti-phishing and anti-spyware technology, secure data backup and sharing, identity protection, ant-botnet tools, DNS security, and privacy protection tools, with an extensive educational program, customer support, and strategic partnerships with related industry experts. It also provides brand-new protections designed to address the growing bot problem by integrating anti-keystroke logging technology with a secure login.

Unlike traditional anti-virus approaches that focus solely on protecting the computer or device, the Constant Guard Protection Suite (see screen shot below), one of the Constant Guard system's components, protects the user's personal information and privacy by concealing typed characters, safeguarding credit card information, protecting and remembering passwords, and providing one-click secure login to financial, commercial, and any other online accounts. The range of features and software offered in the Constant Guard system is offered to all of Comcast's Xfinity Internet customers at no additional cost.



Irrespective of whether a subscriber installs any software from Comcast, we also strive to identify computers infected with malware that are operating in bot networks. Once detection has occurred, Comcast employs a graduated notification process for alerting subscribers with devices that may be infected by a bot, alerting users first via email and then, if the problem persists, through browser notification, such as the example provided below:

xfinity CLOSE X

Constant Guard™ Alert

Your immediate attention is required.

Constant Guard from XFINITY identified that one or more of your computers may be infected with a 'bot'. Please visit XFINITY.com/BotAssistance by clicking the '**Get Help Now**' button for important information on how to remove malicious software from your computer(s).

GET HELP NOW

How do I know this is from Comcast?

Message by Comcast.

These alerts have also been customized to specific types of malware, such as the DNS Changer malware that was the focus of the Federal Bureau of Investigations' recent Operation Ghost Click.

xfinity Show Me What Malware I Have

Constant Guard™ Alert

Critical Malware Alert - Immediate Action Required!

Constant Guard™ from XFINITY detected that one or more of your computers are infected with malicious software that modifies your computer settings. Action must be taken before **March 6, 2012** to avoid disruption to your Internet service.

Please follow the instructions listed on Xfinity.com/dnsbot by clicking the Get Started button below.

GET STARTED

How do I know this message is from Comcast?

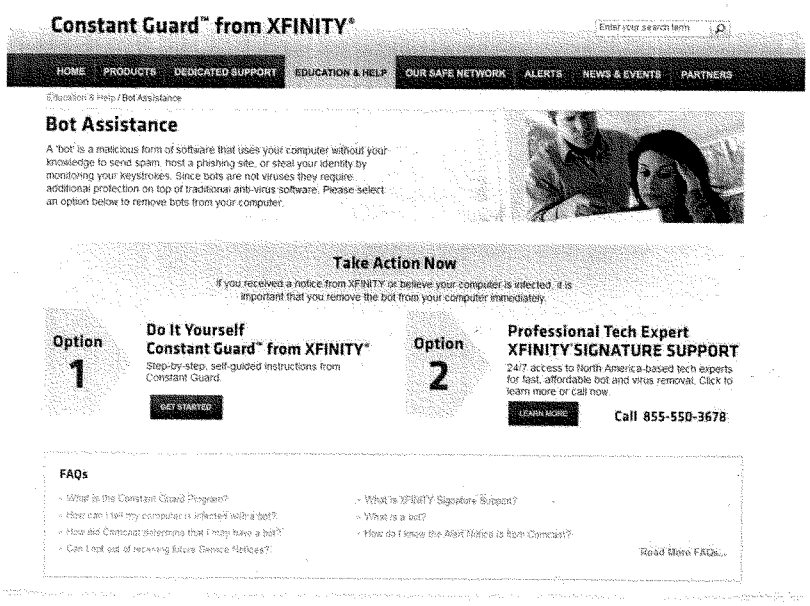
Message by Comcast.

Infected users are directed to the Constant Guard Center web site[5] where they can find the resources needed to safely remove the malicious bot. Once there, subscribers can avail

[5] http://xfinity.comcast.net/constantguard/botassistance/

themselves of either of two types of solutions: (1) a do-it-yourself option with step-by-step, self-guided instructions; or (2) access to round-the-clock U.S.-based technical experts on bot and virus removal.

This screen shot shows what the Constant Guard Center looks like, followed by what a user can discover about the malware they have:



xfinity Home TV Connect Account Shop Help | Security

Constant Guard™ - "Am I Botted?"

Site Navigation: Am I Botted? Home | Am I Botted? FAQs | Results

Constant Guard™ from XFINITY has identified that one or more of your computers may be infected with a bot.

For your IP address the following botnets have been seen in the last week. Options

Botnet	Intent	Severity	MSRT Fix	Last Seen	Times Seen	Advisory
BlackEnergy2	DDoS	64	Yes	2012-02-13 11:36:43 Local Time	15	-
Bredolabs	Multi-Purpose	75	Yes	2012-02-13 11:36:43 Local Time	62	-
Cutwail_Group_A	Spam	64	Yes	2012-02-13 11:36:43 Local Time	12	-
DNS CHANGER	Multi-Purpose	100	Yes	2012-02-13 11:36:43 Local Time	8	Immediate Action required. Visit http://dns-changer.com/ for remediation instructions.
Rogue_AV_Group_C	Multi-Purpose	60	Yes	2012-02-13 11:36:43 Local Time	4	-

Act Now: Visit the Constant Guard™ Bot Assistance Page for remediation instructions.

Comcast recognizes that consumer-based security tools need to work in conjunction with network-based measures to help secure networks and safeguard end users from cyber threats. Comcast has invested substantial resources to deploy state-of-the-art technologies and applications to secure its network.

Comcast's DNSSEC Deployment

The Domain Name System (DNS) is responsible for translating host names (like www.comcast.com) to Internet Protocol addresses (the addresses used by computers to route Internet traffic around the world) and it is critical to the normal operation of Internet-connected systems. Domain Name System Security Extensions (DNSSEC) is an enhanced level of Internet security that ensures the authenticity of the sites that consumers seek to access when they type

domain names into their browsers for example, and prevents them from being unwittingly directed to fraudulent replicas of those sites.

Comcast this year became the first ISP in North America to fully implement DNSSEC. Comcast's decision to deploy DNSSEC has its origins in the 2008 discovery of what has come to be known as the "Kaminsky Vulnerability." In July 2008, Dan Kaminsky, a security expert, announced the discovery of a serious and fundamental security vulnerability in the DNS. The so-called "Kaminsky Vulnerability" is a flaw that affects the way DNS servers handle requests to translate words into numbers, allowing knowledgeable hackers to trick the servers into redirecting web surfers and other Internet users to malicious web sites, among other risks. What made Kaminsky's discovery all the more troubling is that the flaw is not just a bug unique to a single platform; it is a fundamental design flaw in the DNS protocol itself, which allows attackers to easily perform "cache poisoning" attacks on most nameservers on a widespread basis.

DNSSEC essentially patches the security hole in the DNS that was exposed by Kaminsky. Without DNSSEC, the dangers to ISPs and their end users from this security vulnerability are numerous. Left unresolved, hackers could, for example, operate "phishing" scams or "man-in-the-middle" attacks, in which users are directed to fake web pages for supposedly legitimate banks or businesses where they are tricked into disclosing sensitive personal data, including credit card and banking information. Web traffic, email, and other important network traffic can be redirected to systems under an attacker's control, where it can then be used for a wide variety of criminal activities. Users can be led to download unwittingly malware that threatens not only their personal information and devices, but also the integrity of an ISP's whole network.

In response to Kaminsky's discovery, Comcast not only patched its systems prior to the public announcement of the vulnerability, but also immediately started to investigate deploying DNSSEC. We launched a DNSSEC trial in October 2008 to understand and document the steps that ISPs and other implementers should undertake to implement DNSSEC-capable resolvers widely across large-scale networks. In February 2010, we expanded our trial to all production network DNS server locations across the country. Comcast performed this upgrade at the same time that it was upgrading its systems to handle IPv6, the next generation of IP addressing, which is something many other ISPs are doing now as well. Later that year, the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, Inc. collaborated to deploy a signed DNS root zone, a seminal step in enabling DNSSEC globally. This in turn enabled Comcast and other ISPs to be in a position to begin to validate names using an official and public root rather than a temporary one for testing. After that, many top-level domains (TLDs) such as .COM, .NET, .ORG, and .GOV followed suit and signed their respective TLDs, enabling us to both sign domain names in DNSSEC-enabled TLDs, and to perform DNSSEC validation when our customers seek to access a web site or other domain name-based Internet resource.

ISPs play two critical roles in DNSSEC. The first is to validate DNSSEC as part of the DNS lookups performed for users. These lookups occur when a customer tries to access a site, such as www.comcast.com or www.paypal.com. When a Comcast customer tries to connect to that web site, a Comcast DNS server checks that domain name, and verifies the signature to ensure that it is valid and has not been tampered with by hackers. A customer will only be connected if this security verification has been passed, which occurs so quickly our customers do not even notice that it's being done.

The second role is to cryptographically sign the domain names that the ISP owns (such as www.comcast.com and www.xfinity.com), so that when customers or others using DNSSEC try to connect to services in those domains, they can validate the security of the associated DNS responses. ISPs typically own or manage thousands of domain names.

DNSSEC will help to enhance the security of our customers' Internet experience. But its real impact will be felt as it becomes comprehensively deployed across the entire Internet ecosystem. To that end, Comcast has been actively engaged in industry-wide efforts to encourage others to adopt DNSSEC. On behalf of Comcast, I have been actively involved in the Federal Communications Commission's Communications Security, Reliability and Interoperability Council ("CSRIC") Working Group 5 on DNSSEC Implementation Practices for ISPs. ICANN, the Internet Engineering Task Force (IETF), the Internet Society (ISOC) and many other groups are also working hard to make DNSSEC adoption a top priority across the Internet ecosystem.

Accelerating the rate of DNSSEC adoption by ISPs is not without challenges. There are operational procedures, network equipment, and software that may need to be adjusted or upgraded to support DNSSEC validation, and some companies may perceive the immediate costs of implementation to outweigh the rewards. There are other challenges to be faced as well. For example, in the past six months we have experienced several instances of .GOV domains with serious errors in their authoritative data, causing affected domain names to fail DNSSEC validation, which made these sites unreachable for our customers until those domains were fixed by their administrators. These were not always easy to resolve, as establishing the contact information and an escalation path for domains in the .GOV TLD, as with all other domains, can be fairly challenging (due in part to deficiencies in WHOIS-based data, an issue that is getting

attention within ICANN). In addition, the .GOV domain infrastructure could be more closely monitored in order to identify and rapidly resolve DNSSEC validation in a coordinated fashion rather than having each ISP inefficiently trying to notify domains and track these issues to resolution on their own (there are some efforts in these areas, but they may need more resources). The problems associated with the .GOV TLD are not uncommon for early adopters of any new technology, especially considering that the rate of .GOV DNSSEC adoption is actually quite high compared to other TLDs. This will be an issue that will occur as more domains sign, so it is important for the Internet community to foster good, reliable, and repeatable domain signing practices, which will clearly enhance the security benefits associated with DNSSEC deployment.

Comcast has worked hard to be a leader with our DNSSEC deployment. As of today, over 18 million residential customers of our Xfinity Internet service are using DNSSEC-validating DNS servers. In addition, all of the operable domain names owned by Comcast, numbering over 5,000, have been cryptographically signed.

The expansive deployment of DNSSEC unquestionably will help to foster a more secure environment on the Internet, but we are only too aware that cyber threats are ever-changing. The growing sophistication, number, and scale of cyber threats underscores the importance of ensuring that ISPs and other key players continue to have considerable flexibility to address and respond to those threats, and to be able to do so as rapidly as possible. As important as DNSSEC is, it is just one of many resources available to improve security on the Internet.

Comcast's Participation in Public-Private Cybersecurity Initiatives

In addition to investing in network-based security tools and consumer-oriented offerings, Comcast has taken an active role in industry-wide and public-private initiatives aimed at addressing key cybersecurity issues on a systemic level. Comcast is an active participant in the

FCC's CSRIC, which serves as an important forum for developing best practices and voluntary mechanisms for ISPs to meet cybersecurity threats (and other issues). Comcast personnel are currently participating in several CSRIC working groups focusing on issues like Network Security Best Practices (CSRIC WG 4), DNSSEC Implementation and Practices for ISPs (CSRIC WG 5), Secure BGP Deployment (WG 6), and Botnet Remediation (WG 7, chaired by Comcast Fellow, Michael O'Reirdan).

Comcast is also a sponsor-level member of the Messaging, Malware, and Mobile Anti-Abuse Working Group ("MAAWG"), which is also chaired by Mr. O'Reirdan. MAAWG is the industry's largest global trade association that works against messaging spam, malware, viruses, denial-of-service attacks, and other online exploitation. MAAWG has been particularly active in developing voluntary practices that could serve as a framework for botnet remediation. It has published several reports and comments on the issue, drawing from technical experts, researchers, and policy specialists from a broad base of ISPs and Network Operators representing over one billion mailboxes, as well as from key technology providers, academia, and volume sender organizations. MAAWG is currently engaged in a comprehensive effort to develop a program that will gather true cross-ISP bot infection metrics. The MAAWG metrics will help scope the size of the problem, and measure the success of the industry's efforts to combat it.

In addition to its involvement in these groups, Comcast is participating in an ongoing anti-botnet initiative, spearheaded by the Administration, to initiate a multi-stakeholder process aimed at developing a set of common principles for addressing botnet issues. This effort is aimed particularly at highlighting the most effective practices and protocols related to botnet detection, mitigation, and remediation, as well as consumer education. There have also been discussions centering on strategies for targeting criminal behavior, including ways to reduce

recidivism, increase the effectiveness of botnet takedowns, and decrease the number of botnet command and control servers, as well as the number of messages conveyed between the servers and infected machines.

Comcast is also involved in a range of other organizations where security practices are discussed or worked on in other ways, including the North American Network Operators' Group (NANOG), the joint FBI-industry group InfraGard, and the Domain Name System Operations Analysis and Research Center (DNSOARC), among others. And I personally serve on ICANN's Security and Stability Advisory Committee (SSAC), as well as on the Board of Trustees of ISOC, which has been instrumental in supporting key security initiatives like DNSSEC. Comcast also is a founding member of the Broadband Internet Technical Advisory Group (BITAG), which from time to time may touch on security-related work.

Conclusion

As you can see, Comcast has strong incentives – without the need for a government mandate – to explore and implement successfully a wide range of cybersecurity measures. We believe that, to be effective, it is vital that everyone who is part of the Internet ecosystem play a meaningful role in cybersecurity. That includes private and government networks, personal computers and other device makers, application providers, software developers, and others. ISPs and other affected entities must have the flexibility to respond to real-time botnet and other security threats in a manner that minimizes delay, and maximizes initiative and innovation. This is especially true since the threats evolve far more rapidly than any laws or regulatory framework. For example, a few years ago, spam seemed to be a primary focus, but that has now shifted to malware and bots, so organizations must have the freedom to remain nimble and

handle whatever comes next. In addition, the Internet itself is an organic and ever-changing thing, and the pace of innovation within it is amazingly fast.

Thus, flexibility is absolutely necessary in light of the high-velocity changes in technology, business models, service, application vendors, and customer devices employed by each network operator and/or installed by Internet users in their homes or on their devices. Indeed, a government-mandated "one size fits all" approach could actually undermine cybersecurity by allowing criminals and hackers to launch an attack on multiple networks simultaneously if they are able to circumvent uniform or homogeneous detection and deterrence measures, or could constrain the pace of innovation in Internet-related technologies, services, and applications.

In contrast, clarification of the rules for inter-industry and industry-government information sharing on actual or potential cyberattacks would enhance cybersecurity preparedness and response. Information sharing is critical to effective cybersecurity efforts, but it potentially conflicts with statutory provisions, including the Electronic Communications Privacy Act ("ECPA"), the Freedom of Information Act, antitrust restrictions on intercompany sharing of proprietary information, and privacy provisions in the Communications Act. The uncertainty over the applicability of these laws to cybersecurity efforts can create procedural impediments to the timely sharing of relevant information. We support Congress' efforts to review these issues and provide clarification.

The government also should consider embarking upon a consumer education campaign that would utilize Public Service Announcements and other outreach tools to enhance public awareness and understanding of cybersecurity issues in general and bot/malware threats in particular. In addition, special research and development tax credits to encourage the

development of bot/malware-related end user notification and remediation tools, and special tax credit for costs related to notifying and remediating customers affected by malware could also accelerate deployment and adoption of consumer-oriented tools that promote cybersecurity and make network environments safer for all consumers.

Thank you again for inviting me to testify. I would be happy to answer any questions you may have.

Mr. WALDEN. Thank you, sir. We appreciate your comments and we will get back to you with some questions on the specifics of what those uncertainties are in the law.

We now are delighted to have Dr. Edward Amoroso with us. He is the Chief Security Officer for AT&T Services, Inc. Doctor, we are glad to have you here. We look forward to your comments.

STATEMENT OF EDWARD AMOROSO

Mr. AMOROSO. Great. Thanks. Hi, everybody. I am Ed Amoroso. I have spent my entire adult life in cybersecurity. In fact, even as a teenager, my dad was a computer scientist so I was logging onto ARPAnet when I was a little kid. So I have been in and around this forever. I started work at Bell Laboratories and found that I was actually a pretty good hacker, and have been doing so ever since and now I am the Chief Security Officer, so I kind of come at this with very practical perspective on threat.

There are three things I want to share with you that I think are observations that might help you as you develop legislation, and they are based on empirical day-to-day, you know, dealings with security issues with our mobility network and our wireline network and the entire Fortune 1000 and lots of different countries we deal with, so I do that all day long and I wanted to share.

And the first one is about innovation. We are being out-innovated by our adversaries is basically the case. I mean, I don't know if you have ever bought a piece of furniture and taken it home and admired the handiwork in the furniture. That is what we do with malware that is being developed by adversaries. It is so good and so well crafted that we marvel at how far the adversary has come. These are not script kiddies doing dopey things. And these are pretty good. I don't know if any of you watch 60 Minutes, if you saw the Stuxnet piece. That is an incredible piece of computer science, that worm. So I think we need to recognize that whatever we do collectively as a Nation, we need to figure out a way to incent companies and universities and government agencies to innovate in this area. If we don't, we are going to be in trouble because I will tell you, and I bet everybody on the panel here would agree with me, the best state-of-the-art security protections that any one of us can put in place will not stop a determined adversary in 2012. That is a fact, so we need to do something to get ahead of that, and the way you do something is, you innovate. We need to do something to get ahead of it, and part of the problem with sort of prescripting an answer to everyone, hey, we are all going to do the following, is it would be like every NBA team publishing their defense and saying this is what we are going to do. Guess what? You think the adversaries don't read your legislation? You think they don't look and see what we are all going to do? I mean, you lay it out and you say OK, I will step around these things that you are doing. I mean, that is just a practical issue in cybersecurity. This is not, you know, the kind of thing where, you know, we can all kind of do commonsense stuff and it will fix it. There is a million things in our lives where if we all go back to the basics and do a set of commonsense things that will make things better. We all live our lives that way. Cybersecurity doesn't work

that way. We are dealing with an adversary. So the first issue is innovation.

The second is infrastructure, and I think everybody also at this table would agree that complexity in infrastructure is the biggest problem for cybersecurity. When things get way too complicated, we can't keep track of it. It becomes almost impossible to protect something that has become so big and complicated that you can't get your arms around it, and part of the problem with things like DNSSEC and others, which clearly have benefit—I mean, I certainly agree with a lot of the points that were made—but they add complexity. Like the way to think of DNSSEC is, you know when you do a commercial and at the end you say I am such-and-such and I approved this commercial, that is DNSSEC. I mean, it is essentially the server attesting to the fact that here is a signature that I am who I am, but if somebody is breaking in to and owns that server, the signature is meaningless. It doesn't do any good. And I would say empirically, I see a lot more break-ins to DNS servers than forged, you know, different types of protocol responses and so on. So I think what we need to keep in mind as we develop legislation that when we add complexity, when you add things that we need to keep track of, do this, do that, overlay this, add this new thing, add that new thing, the complexity can be very stifling. You know when DNSSEC was first proposed? Decades ago. Right. This is not something that was dreamed up last week. We have been working on adding cryptography to Internet protocols forever, and the reason we don't have them today is because they are unbelievably complicated to run. They do add some benefit but they have side effects. It would be like bringing a senior citizen to the doctor with five ailments and the doctor says well, I am going to give you medicine for one of them but it has side effects. That is DNSSEC. It does have benefit, it has side effects, it doesn't fix everything, so that is the second.

The third and last issue I want to raise is software. At the root of every cyber attack, every problem I have ever dealt with in my entire career is bad software, and I think that it needs to be addressed. The discipline of software engineering, the profession of writing software is one that is a complete mess right now. And I am a professor at the Stevens Institute of Technology. I have been teaching in the computer science department there for 22 years. I teach software engineering, teach computer security, that kind of thing, so maybe blame me, but the bottom line is that youngsters and even professionals today cannot write a non-trivial piece of software that is bug-free and those bugs are the way our adversaries get into our companies. We open up Web sites because we have no choice. Are we going to close the Web site down? It is there and the software powering that has vulnerabilities we don't know about. I bought it, I install it, I test it, everything is great, but some adversary finds an open door that I don't know about, that the manufacturer doesn't know about, and they dance right in. Bad software is a fundamental problem here, and I think it needs to be addressed, probably through the educational system. Thanks.

[The prepared statement of Mr. Amoroso follows:]

Statement of Edward Amoroso, Ph.D.

Senior Vice President & Chief Security Officer
AT&T

Hearing: Cybersecurity: Threats to Communications Networks and Private-Sector Responses

United States House of Representatives

Committee on Energy & Commerce
Subcommittee on Communications and Technology

March 7, 2012

Chairman Walden and Ranking Member Eshoo, I would like to thank you and all the members of the Subcommittee for this invitation to address the significant challenges facing communications networks in particular, and the private sector in general, with regard to effectively defending against cyber threats. In this statement, I briefly describe cyber threats and cybersecurity, and discuss generally how federal legislation under consideration in this Congress could be fashioned to both enhance the private sector's cybersecurity practices and facilitate greater coordination between the cybersecurity capabilities of the federal government and the private sector.

My Background

I am Senior Vice President and Chief Security Officer, AT&T, where I have worked in the area of cybersecurity for the past twenty-seven years.[1] With the help of my team, I design and operate the security systems and processes that protect AT&T's domestic and international

[1] I hold a Bachelors degree in Physics from Dickinson College, both a Masters degree and the PhD in Computer Science from Stevens Institute of Technology, and have served as an adjunct professor of computer science at Stevens for the past twenty-three years. I am a graduate of the Columbia Business School, and the author of numerous articles and books on cybersecurity, including "Cyber Attacks: Protecting National Infrastructure" (Butterworth-Heinemann, 2011).

wired and wireless network infrastructure. This network infrastructure is the core asset that permits AT&T to provide an array of advanced communications services to many millions of customers around the world, ranging from the largest global business and government enterprises to small businesses and individual consumers. The technologies provisioned and employed by AT&T and the other communications network providers represented here today are a key part of the national infrastructure – the complex delivery and support systems for the large-scale services that are essential to the commercial security of our nation.

What is cybersecurity, and what are today's cyber threats?

National infrastructure, including the communications infrastructure, have always been vulnerable to direct physical attacks such as cable cuts, asset theft, equipment tampering and even more violent forms of sabotage. As elements of this infrastructure became increasingly reliant on software, computers, networks, and access to the Internet for their control systems, they became correspondingly vulnerable to indirect "cyber" attacks by adversaries[2] intruding these computerized control systems. Cybersecurity is the term we use to describe an entity's ability to protect its critical systems from these intrusions by monitoring its systems in order to detect cyber threats and then engage in "active defenses" to mitigate those threats. In addition, the forensic results of this activity might be usefully shared with others, within appropriate parameters, so that others might leverage the experience and knowledge acquired in order to further protect their infrastructure from intrusion.

The methods and forms of cyber attack threats are continuously evolving, and this dynamism enables such threats to bypass standard preventive measures such as the application of

[2] Sources of cyber threats include (but are not limited to) disgruntled individuals, criminal elements, transnational enterprises, and sophisticated and well-resourced nation states. These sources are motivated by a range of purposes, from mischief to deliberate acts of hostility attempted through sabotage and terrorism.

firewalls and intrusion detection systems strategically placed between the critical system and the Internet at large. One form of evolving cyber attack uses "botnets" – which are run by adversaries who are increasingly adept at harnessing the power of dispersed personal computers and other smart devices attached to the national infrastructure and using them to attack unsuspecting victims. Other cyber threats include worms, viruses, and leaks, which can similarly target national infrastructure through their associated automated controls systems. All of these threats can be employed by adversaries to engage in a range of conduct from Distributed Denial of Service Attacks (DDOS) to Advanced Persistent Threats (APT), which are at present the most sophisticated and pernicious forms of cyber attack.

What needs to be done?

We need to improve the overall cybersecurity posture of the nation by facilitating the widespread and rapid adoption of cyber threat detection and mitigation practices through private sector investment and innovation. Because of the global nature of the threat, we cannot undertake this challenge unilaterally – it is clearly a global issue in all its dimensions. The Administration and the Congress have put forth a variety of ideas and initiatives on how we can begin to tackle this challenge; some are helpful, and some would stifle the innovation and flexibility we need to identify and respond to the ever changing threats. AT&T commends, in particular, the work of the Cyber Security Task Force and the leadership of Congressman Mac Thornberry. The Task Force produced a focused set of recommendations that should be used as the framework for any proposed cyber legislation. Implicit in the Task Force recommendations is the principle that improving our national cyber security posture is a process that will not be solved by simple legislative pronouncements or regulatory dictates. We can, however, begin to establish foundational elements for future progress.

1. **Build a Collaborative Active Cyber-Defense Capability.**

First and foremost, the United States needs to build a collaborative active cyber-defense capability that builds upon well-established coordination processes that have been developed for assessing cyber threat risks to critical infrastructures and key resources (CIKR). Our experience participating in these processes, as well as in pilot programs such as the Defense Industrial Base (or "DIB") Project, informs our view that more targeted cyber threat information sharing capabilities to support active cyber defense should be the next step in our nations approach to securing its infrastructure.

To this end, the global communications infrastructure is the primary vehicle for delivery of cyber attacks against U.S. interests, yet there is no comprehensive coordination mechanism for rapidly detecting and analyzing emerging threats. Each Tier One communications network operator and service provider monitors its own network to varying degrees, with varying capabilities to mitigate or block attacks. In addition, the multiple government programs which already exist are focused on monitoring traffic to and from multiple government networks – none of which are operationally integrated.

Actionable emerging threat information might be known to the Federal Government, for example, but otherwise unknown to private industry. In the event that a government agency becomes aware of a malicious attack signature that could be deployed into intrusion detection systems to protect industrial, non-government assets, the government should have the confidence that it can be so deployed without further delay or review. A collaborative, active cyber-defense capability to detect, analyze, and mitigate malicious cyber activities in the core networks that make up the Internet itself will enable cyber attacks to be detected and attempts be made to stop them before they reach their target.

This Congress there have been a number of legislative proposals that appear to be an excellent first step toward achieving the end goal of a collaborative active cyber-defense capability by explicitly authorizing cyber threat information sharing between private and public sector participants, as well as the active defenses or countermeasures necessary for entities to engage in so that they can address those threats, either for themselves or on behalf of others. In particular, we note H.R. 3523, the Cyber Intelligence Sharing and Protection Act, introduced by Michigan Congressman Mike Rogers. This proposal has done much to advance the discussion of the appropriate range and scope of cybersecurity activities and threat information sharing among all stakeholders.

An important component of these more recent proposals is statutory clarity with regard to an entity's lawful authority to monitor, use and disclose cyber threat information for cybersecurity purposes in the first instance, as well as corresponding market incentives, such as liability protection, for entities that engage in active cyber defense. I cannot overstate the importance of such clarity to speeding the more rapid adoption of effective cybersecurity practices, and the significance of the paradigm shift that we see taking place. Until stakeholders, including lawmakers, fully appreciate and understand that the monitoring, use and disclosure activities engaged in by cybersecurity providers are largely limited to non-content metadata, and are undertaken solely to defend network systems and assets against cyber attacks, then terms like "monitor," "use," and "disclose" – will continue to be viewed with apprehension even in the context of legitimate cybersecurity.

This apprehension, we believe, is manifested in the current, complicated legal and regulatory environment in which cybersecurity is practiced. This environment necessarily compels significant lawyer involvement in various aspects of the provision of cybersecurity

services. This need for near-continuous legal consultation necessarily inhibits the more rapid and widespread adoption of robust cybersecurity practices by private sector firms. However, if carefully circumscribed cybersecurity activities were to be clearly defined in functional, non-legalistic terms in a federal statute for which cybersecurity professionals need not resort to legal consultation and interpretation as a matter of course, then we believe entities will more readily adopt cybersecurity practices and more-readily share cyber threat information.

As to those proposals that bear on the establishment of a national, collaborative active cyber-defense capability, we believe that many of the "information sharing proposals" under consideration in Congress have made a sound start in this regard by establishing a basis for the Federal Government to more routinely share classified threat warning information with appropriate private sector entities as well as to permit such private entities to share threat information with each other. In our own case, AT&T leverages the intelligence of its advanced global network, coupled with sophisticated behavioral analysis techniques, to detect attacks while they are still in the development stage, and to rapidly implement protective measures for ourselves and our customers. By joining these capabilities with those of the other carriers/service providers, along with those of the security and software companies, we can create a capability to identify cyber threats as they emerge, and to rapidly mitigate them. This leveraging of existing private sector capabilities and "fusing" them with the classified threat warnings that only the Government can provide should be central to any legislative proposal on cyber threat information sharing. We look forward to working with stakeholders on ways to ensure that federal cybersecurity legislation will enable this end.

2. **Government Leadership.**

The United States government must lead by example in cyber security. The federal government is the largest single purchaser of information technology and network services in the United States, and its leadership and buying power can have great influence on the cyber security marketplace. Several worthwhile federal initiatives are in place to improve cyber security for the ".gov" domain, such as the Trusted Internet Connection effort by the Office of Management and Budget (OMB) and the advanced security service carriers offer Federal agencies through the General Service Administration/Department of Homeland Security joint initiative on Managed Trusted Internet Protection Service (MTIPS), but they are being applied inconsistently throughout the government. These initiatives could be expanded throughout the Federal Government in order to provide better cyber security at lower cost. By integrating MTIPS and like-managed cyber security services with the advanced cyber threat detection capability discussed above, our entire critical infrastructure can be more effectively and efficiently protected against the full range of cyber threats.

The Department of Defense also has its own effort to protect ".mil", separate from the ".gov" efforts. These initiatives do not yet take full advantage of the portfolio of managed security services offered by many private sector network service providers, such as network-based protection against DDOS attacks. The federal government needs a clear and comprehensive strategy for cyber security of all Federal systems that make up ".gov" and ".mil" - one which effectively leverages existing cyber security capabilities offered by the network service providers.

Further, the current roles and authorities of the various federal agencies overlap and are unclear with respect to cyber security for federal government infrastructure. Congress can lead

by establishing discrete, definitive roles and authorities of the various Executive Branch elements involved in all aspects of cyber security – including the National Security Council and the Cyber Policy Coordinator, the Office of Management and Budget, the Office of Science and Technology Policy, the Department of Homeland Security, the Department of Commerce including the National Institute of Standards and Technology and the National Telecommunications and Information Administration, the Department of Defense including U.S. Cyber Command and the National Security Agency, and the Department of State. The United States needs a unified Federal government effort on cyber security with a clear understanding of the roles involved – not the confusion that currently exists.

Happily, a number of the pending legislative proposals seek to address the problem of duplicative or redundant roles and authorities, and seek to establish other government cyber reform, particularly with regard to reforming the Federal Information Security Management Act of 2002, or FISMA. A number of proposals are properly focused on cyber awareness and cyber education, as well as work force development and cybersecurity R&D. The federal government can help to improve overall cybersecurity by promoting the creation and adoption of cybersecurity-oriented curriculum in schools, as well as work with the private sector to facilitate cybersecurity education and research.

Indeed, we all must redouble our efforts in cyber security education and awareness across the full spectrum of the Internet user base – from the boardrooms of our largest companies to the millions of individuals who surf the 'net. Current efforts in cyber security education and awareness are fragmented and the messaging is often confusing. The ultimate key to improving our national cyber security is technology innovation driven by market demand from informed users and purchasers of all kinds. By creating market demand for cyber security through

heightened consumer awareness, we can spur fundamental security innovation at all levels of the Internet eco-system, and allow the United States to continue as a leader in Internet development.

To that end, Congress should consider designating a lead Agency on cyber security education, and support that designation with an appropriate level of funding to make it effective. The roles of other Federal Agencies in supporting this effort should also be clarified. One of the key struggles in cybersecurity at the individual consumer level is the low rate of user adoption of proven protection mechanisms. This is one area where the government could positively influence the trajectory of cybersecurity by engaging in a comprehensive education and outreach campaign to inform consumers about security best practices and how to protect themselves and their sensitive information.[3]

3. Global Strategy.

As I mentioned at the outset, cybersecurity is a global issue in all its dimensions. The United States must move forward aggressively to create a comprehensive strategy for addressing global cooperation in cyber security. We must reinforce the leadership of the United States in shaping the future of the Internet, and assuring its stable, reliable, and secure operation, as U.S. enterprise expands in the global Internet marketplace. In particular, all members and participants of the global Internet community must achieve consensus on the fundamental point that malicious cyber activities of any sort will simply not be tolerated. Federal legislation should at least attempt to address the global context of cybersecurity by establishing a framework for international cooperation in this regard, particularly in the establishment of international

[3] AT&T is itself actively engaged in the provision of cyber security information and protective tools to our customers, and actively participates in pan-industry cyber awareness education efforts such as "Stop.Think.Connect," the coordinated messaging effort spearheaded by the Anti-Phishing Working Group and the National Cyber Security Alliance and comprised of government agencies, private sector entities, and not-for-profit corporations.

agreements that will enable real-time global coordination in addressing cyber attacks. Concurrent with these efforts, Congress should also expand incentives for investment by the private sector to help invigorate U.S. technology leadership in cyber security and the Internet.

When legislation has the potential to hinder, rather than help

1. Unintended Consequences of Regulation

Some cybersecurity legislative proposals include a variety of regulatory schemes, ranging from standardized certification regimes to processes that could result in the imposition of regulatory performance standards on some critical infrastructure sectors, including the communications sector. Such proposals, while undoubtedly well-intentioned, are the antithesis of innovation – such requirements could have an unintended stifling effect on making real cyber security improvements. Cyber adversaries are dynamic and increasingly sophisticated, and do not operate under a laboriously defined set of rules or processes. The challenges we face in cyber security simply cannot be solved by imposing slow moving, bureaucratic processes on those who build, operate in, and use cyber space. Overbroad regulation and certification requirements will likely have unintended consequences, such as emphasizing the status quo by focusing on yesterday's challenges. An overly prescriptive approach can only serve to stifle Internet innovation and the technology leadership of the United States in the global information infrastructure. Quite simply, innovation is inconsistent with standardization.

I have heard it observed that federal cyber regulation is needed because no one firm in the private sector has the financial incentive to invest in capabilities to address a cyber incident that affects more than the value of the assets of that firm. Even if this were true, the answer is not for government to prescribe regulatory patches on discrete elements of the various critical infrastructure sectors in the hopes that these patches will effectively deter ever-evolving

intrusions by cyber adversaries. Rather, the answer is for government to facilitate the creation of the most effective cybersecurity tools possible and to permit the private sector to respond to emerging threats in diverse and innovative ways.

Conclusion

Private sector investment and innovation has made the Internet ecosystem the success it is today, and drives the dynamics of the technology and how it is used in global business and the operation of our critical infrastructure. AT&T invests in our network and leads innovation in cyber security because it is in our customers' interests to do so. We want to be a leader in cyber security, as well as all the other aspects of our business, because we understand the competitive advantage such leadership provides in a highly competitive global marketplace. We strongly believe that the most effective way to move forward on cyber security is to broadly spur investment and innovation, based on increased awareness of cybersecurity by the CEOs of the largest companies to the individual consumers that drive market demand.

The Internet itself was created through innovation. Some key early investments by the government helped spur that innovation. Congress and the Administration have leadership rolls to play in assuring that the United States continues to focus on technology innovation. Burdening the private sector with the cost of unnecessary and ineffective regulations and processes is contrary to that objective, and will only slow advances in cyber security. Congress must insist on and support initiatives that provide the flexibility needed to deal with the dynamics of the threat and the technology, while creating innovation and investment through market demand.

I thank the Subcommittee for its timely and focused attention on cybersecurity, and I look forward to providing on-going guidance, assistance, and recommendations as we collectively work to reduce the cybersecurity threat to our nation and our critical infrastructure.

Mr. WALDEN. Thank you. We appreciate your comments and we will back to you with questions as well.

Now we are joined by Mr. David Mahon, Chief Security Officer for CenturyLink. Thank you for being here. We look forward to your comments.

STATEMENT OF DAVID MAHON

Mr. MAHON. Chairman Walden, Ranking Member Eshoo and members of the subcommittee, thank you for the opportunity to testify on this important topic.

CenturyLink, a tier one backbone provider, provides communication services to over——

Mr. WALDEN. We are having trouble hearing you. Is that light lit up there, and you really have to get really close.

Mr. MAHON. Chairman Walden, Ranking Member Eshoo and members of the subcommittee, thank you for the opportunity to testify today on this important topic.

CenturyLink, a tier one backbone provider, provides communication services to over 14 million homes and businesses in more than 37 States and around the world. Our services include voice, broadband, video entertainment and data, as well as fiber backhaul, cloud computing and managed security solutions. Our customers range from the most basic voice and Internet customers to the largest Fortune 500 companies and large government agencies. As Vice President and Chief Security Officer for CenturyLink, I am responsible for all corporate security functions including information security.

Before joining CenturyLink, I worked for over 30 years with the FBI and was responsible for investigative teams and programs related to target attacks on the Internet, computer systems and networks exploited by terrorist organizations, criminal and intelligence operations of foreign governments, white-collar crime investigations, and crisis management.

The cyber threat is real and serious. Our networks and those of our customers are the targets of thousands of cybersecurity events daily from simple port scans probing network defenses to sophisticated attacks. CenturyLink and our customers invest significant resources in ongoing efforts to keep those assets secure. CenturyLink uses an overarching governance, risk and compliance framework to ensure cybersecurity threats are addressed enterprise-wide. As stewards of the Internet infrastructure, CenturyLink's programs on cybersecurity fall into several general categories: protecting the customer, protecting our core networks and providing managed cybersecurity and secure communication services.

We have worked extensively with our industry peers, partners in government and other stakeholders to strengthen our collective defenses against cyber attacks. From our CEO's participation on the President's National Security Telecommunications Advisory Committee to my security team's participation in key organizations such as DHS's Communication Sector Coordinating Counsel and the FBI's Domestic Security Alliance Council, we conduct risk assessments, information sharing, incident response planning and participate in government-sponsored cybersecurity exercises.

In addition, CenturyLink's CEO, Glen Post, chairs the FCC's Communications Security, Reliability and Interoperability Council, which is working on voluntary best practices for botnet remediation, Domain Name System Security, Internet route hijacking, and other emerging issues unique to the communications industry.

More can and should be done, but carefully. Public-private partnerships have yielded significant progress in the last few years by building a framework of collective defense and cooperation and helping us understand the cyber threat. As many of you have pointed out, we are entering into a new era of cybersecurity threats where our adversaries have become more sophisticated and determined, and the need to collectively step up our game is more acute.

We are particularly encouraged by legislation like H.R. 3523, the Cyber Intelligence Sharing and Protection Act, and similar provisions in Senate bills that could clarify and enhance cyber-related public-private information sharing.

As communication providers, we see a number of areas where Congressional action can make valuable improvements to our Nation's cybersecurity process such as improving information sharing, market-based incentives and gap analysis, improving the Federal Government's cybersecurity posture, and expanded research and development.

Shifting to a mandated-based approach would be counterproductive. We strongly caution against the traditional regulatory approach based on government mandates or performance requirements. Because our network is the one central asset of our business, CenturyLink and our industry peers already have the strongest commercial incentives to invest in and maintain robust cybersecurity. There is neither a lack of will nor a lack of commitment to do this among the major communications providers.

At its best, cybersecurity is a dynamic, constantly evolving challenge best done in a collaborative partnership. At its worst, cybersecurity can devolve into a checklist exercise and diverts resources away from effective protections into expensive compliance measures that may be already outdated by the time they are implemented. We have the most knowledge of our network systems and databases, and we understand the most effective and efficient ways to protect these assets.

We commend the members of the Energy and Commerce Committee for their interest in improving the Nation's cybersecurity and for the deliberate process the committee is undertaking to find the right mix of incentives and elimination of legal barriers. CenturyLink has strived to be a constructive partner in this effort, and we will continue to do so. Thank you.

[The prepared statement of Mr. Mahon follows:]

Testimony of David Mahon
Vice President and Chief Security Officer, CenturyLink, Inc.
before the
Subcommittee on Communications and the Internet
Committee on Energy and Commerce
United States House of Representatives

Wednesday, March 7, 2012

Chairman Walden, Ranking Member Eshoo and members of the Subcommittee, thank you for the opportunity to testify today on this important topic. CenturyLink provides communications services to over 14 million homes and businesses in more than 37 states and around the world, including voice, broadband, video entertainment and data services, as well as fiber backhaul, cloud computing and managed cybersecurity solutions. Our customers range from the most basic voice and internet customers, to the largest Fortune 500 companies and multiple, large government agencies.

As Vice President and Chief Security Officer for CenturyLink, I am responsible for all corporate security functions including information security, critical infrastructure protection, physical security, network fraud, industrial security, workplace violence prevention, support for the National Security Telecommunications Advisory Committee (NSTAC) and DHS National Coordinating Center (NCC) as well as liaison with federal and state law enforcement and homeland security agencies.

Before joining CenturyLink, I worked for over 30 years for the FBI and was responsible for investigative teams and programs related to targeted attacks on the Internet, computer systems and networks exploited by terrorist organizations, criminal and intelligence operations of foreign governments, white collar crime investigations, and crisis management.

The cyber threat is real and serious

We are here today because members of this subcommittee and leaders in the communications industry recognize how important the issue of cybersecurity is to securing the nation's critical infrastructure, protecting consumers, fighting crime and protecting national security. Our networks, and those of our customers, are the targets of thousands of cybersecurity events daily, from simple port scans probing network defenses to sophisticated attacks. CenturyLink and our customers invest significant resources in constant and ongoing efforts to keep those assets secure.

The major cyber threats faced by the public and private sector generally fall into four categories: Nation-state sponsored intrusions (also known as "advanced persistent threat"); Criminal, which extends to sophisticated organized crime; "Hacktivism"; and Insider attacks. Reports in the media, and private industry and government studies have documented the extensive threats to corporations, consumers and government agencies.

As a leading national network provider, CenturyLink utilizes an overarching governance, risk and compliance (GRC) framework to ensure cybersecurity threats are addressed enterprise-wide. This GRC framework allows CenturyLink to advance and evolve its information security program to identify, mitigate and remediate risks related to our corporate and customers' data, networks and systems.

The roles of communications providers

Communications providers are just one part of the cyber ecosystem, so our cybersecurity efforts are just one part of a comprehensive effort that includes technology providers, end users, owner/operators of critical infrastructure, and our government partners. As stewards of the Internet infrastructure, CenturyLink's programs on cybersecurity fall into several general categories:

Protecting the consumer experience.
As hackers, criminals and other entities seek to prey on our customers by exploiting the Internet's open architecture, CenturyLink has worked within the Internet community on measures we can take to mitigate this situation. For instance, when we learn from third-party partners that our customers' computers are likely infected with malware that makes them part of a "botnet," we notify the customers and direct them to resources to help them clean up the malware. This is a free program we launched in 2006 to improve our customer experience and minimize abuse of our network. We notify tens of thousands of customers with infected computers each year, and provide education and remediation tools. We have shared our program and experiences with other ISPs globally and are currently working with the industry on voluntary industry standards to help address the overall botnet problem.

For residential consumers, we provide educational material, anti-virus protection, malware notification and self-help mitigation tools, firewall, and parental controls as part of their ISP service. We also offer fee-based services for customers who need assistance keeping their computers running efficiently along with cleaning malware from their systems

In addition, we are actively engaged in addressing issues in Domain Name System (DNS) and Border Gateway Protocol (BGP) security. We are working with stakeholders and other industry partners on new BGP security standards that we hope will help prevent accidental and malicious Internet route hijacking. We have also worked for the past several years on DNS security by improving the monitoring of the current DNS system while working with industry leaders in developing practical implementations of DNSSEC security.

Protecting our core networks.
As a major communications provider, whose customers expect security and reliability, we are ever mindful that our networks are potential targets. Our security protocols continue to evolve with the increasing sophistication of cyber

attacks and include continuous monitoring, testing and upgrades of our practices and infrastructure to protect our networks. We have a direct and strong economic incentive to keep our networks secure and our services available.

Providing managed cybersecurity and secure communications services. CenturyLink provides a wide range of managed security services to a number of critical infrastructure clients, including government agencies, financial services, transportation and energy providers. We also provide national and international secure cloud computing services and diversified, secure communications paths to ensure reliable and available communications access to those services.

Public-private partnerships

CenturyLink has been an operational and collaborative partner with government for more than 25 years and is a Resident Member of the DHS National Coordinating Center. In the past ten years, we have worked extensively with our industry peers, partners in government and other stakeholders to strengthen our collective defenses against cyber attacks. From our CEO's participation on the President's National Security Telecommunications Advisory Committee, to my security team's participation in key organizations such as the Communications Sector Coordinating Council (CSCC), the FBI's Domestic Security Alliance Council (DSAC), and InfraGard Program, our goal is to share the information we can in order to make our network and the entire communications infrastructure more secure and connected.

We are also members of the National Cyber-Forensics Training Alliance (NCFTA), which functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime. Once a significant online scheme is realized, an initiative is developed wherein the NCFTA manages the collection and sharing of intelligence with the affected parties, industry partners, appropriate law enforcement agencies, and other subject matter experts. In addition, we work extensively with our industry peers, operating system developers, and other private security organizations through the Network Security Information Exchange (NSIE) to ensure the security of our network and customer information.

The government has worked to step up its game as well. From President Bush's Homeland Security Presidential Directive 7 (HSPD-7) to President Obama's 2009 Cyberspace Policy Review, our national leaders have been evolving the government response to cybersecurity. Public-private partnerships and stakeholder programs organized through the Department of Homeland Security (DHS), the FCC, the FBI, Department of Defense and other agencies have focused on a number of key areas where industry and government can strengthen each other's efforts. We participate in many of these programs.

- We are currently working with DHS and other agencies to update the 2008 National Sector Risk Assessment, which will identify potential areas for

continued collaboration between government and the private sector to mitigate cyber threats to the communications industry.

- As a resident member of the DHS National Coordinating Council, CenturyLink maintains an employee presence within National Cybersecurity and Communications Integration Center (NCCIC), to coordinate in real time with government partners in the event of a cyber emergency.

- Working with DHS, CenturyLink, and other members of the Communications Sector, helped develop the National Cyber Incident Response Plan (NCIRP). As part of that effort, CenturyLink helped to develop the roles that industry partners would play in the event of a cyber emergency, and is a designated member of the Unified Coordination Group referenced within the plan.

- We have participated in a number of cyber exercises, including the DHS's biennial "Cyber Storm" exercises, and will be participating in the upcoming National Level Exercise (NLE) 2012. Through these efforts, we seek to better understand the roles each party would play, with the goal of refining the incident response plans.

- We are working through the National Institute for Standards and Technology (NIST) and a number of other industry-centric standards bodies to develop standards and best practices on cybersecurity.

- CenturyLink CEO Glen Post chairs the FCC's Communications, Security, Reliability and Interoperability Council (CSRIC), which is working on voluntary best practices for botnet remediation, domain name system security ("DNSSEC"), Internet route hijacking and other emerging issues unique to the communications industry.

More can and should be done – but carefully

Public-private partnerships have yielded significant progress in the last few years by building a framework for collective defense and cooperation, and helping us understand the cyber threat. Additional progress to improve the nation's cyber defenses will come from continued robust commitment to the partnerships and activities that are already underway.

As many have pointed out, however, we are entering into a new era of cybersecurity threats where our adversaries have become more sophisticated and determined, and the need to collectively step up our game is more acute. We are particularly encouraged by legislation like HR 3523, the Cyber Intelligence Sharing and Protection Act, and similar provisions in Senate bills that could clarify and enhance cyber-related, public-private information sharing. As communications providers, we see a number of areas where congressional action can make valuable improvements to our nation's cybersecurity posture as follows:

Improving information sharing
Information sharing with government and between industry can be improved through legislation, with appropriate privacy protections.

- Clarifying that sharing of cyber threat information among private sector entities is permitted and encouraged.
- Allowing government to reasonably share classified information with cybersecurity providers to enhance protection of critical infrastructure.
- Expediting security clearances and space accreditations to support and expand programs that would use classified information to protect information networks.

Market-based incentives and gap analyses
Market-based incentives and gap analyses can incentivize continued improvement among the private sector. For example, providing liability protection and appropriate antitrust safe harbors for cyber threat information sharing, as well as assurances that cybersecurity disclosures to the government won't be used as excuses for more regulation, would help make public-private partnerships more effective. As cyber threats evolve, regularly updating the communications providers on evolving risks and threats would play a critical role in identifying "gaps" between our current efforts and any incremental defenses needed to focus both government and private sector resources more effectively.

Improving the federal government's cybersecurity posture
We believe reforming the Federal Information Security Management Act (FISMA) through deployment of government-wide managed security solutions and a more active management role for DHS, can protect government networks more effectively.

Expanded research and development
Research and development is necessary to develop new methods of threat mitigation. With clearly defined information sharing policies and procedures with liability protections, ISPs can work more closely with both the affected businesses and government to develop innovative new solutions, and deliver them to the market place more quickly.

Shifting to a mandate-based approach would be counterproductive

We strongly caution against a traditional regulatory approach based on government mandates or "performance requirements." Because our network is the one central asset of our business, CenturyLink and our industry peers already have the strongest commercial incentives to invest in, and maintain robust cybersecurity. There is neither a lack of will nor a lack of commitment to do this among the major communications providers.

At its best, cybersecurity is a dynamic, constantly evolving challenge, best done in a collaborative partnership. At its worst, cybersecurity can devolve into a checklist exercise that diverts resources away from effective, evolving protections, into expensive compliance measures that may be already outdated by the time they are implemented. We have the most knowledge of our network, systems and databases, and we understand the most effective and efficient ways to protect these assets. Our goal-oriented approach to cybersecurity strives to ensure the availability and integrity of our networks and the transactions that go across our networks.

Conclusion

We commend the members of the Energy and Commerce Committee for their interest in improving the nation's cybersecurity, and for the deliberative process the committee is undertaking to find the right mix of incentives and elimination of legal barriers. CenturyLink has strived to be a constructive partner in this effort and will continue to do so.

Mr. WALDEN. Thank you, sir. We appreciate your testimony, and now we will move to Mr. John Olsen, Senior Vice President and Chief Security Officer for MetroPCS Communications. Welcome, and we look forward to your comments.

STATEMENT OF JOHN OLSEN

Mr. OLSEN. Thank you, Chairman Walden and Ranking Member Eshoo. It is an honor to appear before you and your colleagues today. I am the Senior Vice President and Chief Information Officer for MetroPCS Communications. I have nearly 30 years of IT experience, and I am responsible for our IT networks.

MetroPCS is a leading provider of unlimited wireless communication services for a flat rate with no annual contract. We sell our services through our own retail stores and independent MetroPCS dealers to retail consumers. We do not sell through business-to-business sales channels or to the government.

Our communications networks use four well-known and established network vendors: Alcatel-Lucent, Ericcson, Cisco and Samsung. We also purchase handsets from well-known and established vendors. These vendors are not our primary network vendors, which mitigates the risk that an embedded handset threat is able to exploit vulnerabilities in our network.

Our communications networks utilize security measures similar to other carriers. We have also adopted measures both physical and logical to protect these networks. We have four IT networks which are critically important to our business. As we will discuss in more detail, we have voluntarily undertaken a number of cybersecurity measures to protect our IT networks, both physical and logical.

Security of these critical networks is very important to MetroPCS. We maintain a comprehensive, holistic, risk-based information security program built on industry best practices covering people, process and technology. We use a combination of hardware and software services. Our security program directives are driven by a formal governance function and include, among other things, centralized policy management, security awareness, training, and internal and third-party monitoring, physical protection, threat identification and vulnerability management as well as intrusion prevention.

We are particularly focused on security at the perimeter of our IT networks and use multi-level security technologies to prevent unauthorized access to our IT networks from both inside and outside our company. We conduct and we have third-party vendors conduct regular network security audits and penetration tests and have standardized on a single provider or all network equipment. Further, our IT networks are broken up into segments with firewalls between critical segments. Our 24/7 monitoring efforts, which are augmented by our cybersecurity partners, can generate hundreds of thousands of potential cyber threat alerts a day but result in just a handful of real threats, which we address immediately. While we cannot say definitely we have never had a cyber intrusion, we are not aware of any significant cyber intrusions or cyber attacks that have been successful at disrupting our IT or communication networks.

In addition, we have also adopted a number of other measures to protect our customer information such as encrypting hard drives, installing virus and malware software, and for a mode access requiring two factor authentication. We also conduct background checks, segregate duties of personnel and log all access and changes to critical systems. MetroPCS has also implemented numerous physical security measures such as card key and biometric access.

Our staff also maintains vendor-specific and industry-recognized certifications and regularly participates in vendor-sponsored symposiums, industry summits and conferences. We are involved in these groups, not because we are required to but because they are a valuable source of information and best practices.

MetroPCS does not believe that regulation is required or warranted at this time, particularly for carriers that do not provide services to government or local public safety organizations. Carriers are already well incented to protect their networks, and this is particularly true for month-to-month service providers like MetroPCS. If we do not provide the level of protection our customers want or demand, they can terminate service without penalty and can activate service with a competitor. Governmental regulations and private sector certifications such as PCI also force providers to invest in the appropriate tools and practices to detect and deter cyber threats.

Market forces are better suited to respond to constantly changing cyber threats. If regulations are considered, MetroPCS urges that these requirements be flexible and tailored to the threat. Regulatory compliance can be particularly burdensome for carriers who compete by providing an affordably priced differentiated service for consumers.

Unfortunately, even voluntary obligations can evolve into a mandate on industry. We support voluntary industry efforts, industry standard bodies, enhanced governmental consumer education and the FCC's cybersecurity stakeholder efforts along with government sharing of cyber threat intelligence including a national central clearinghouse. Finally, no carrier should be liable for using such information.

Thank you again for the opportunity to testify and I look forward to any questions that you may have.

[The prepared statement of Mr. Olsen follows:]

STATEMENT

Of

JOHN J. OLSEN
SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER
METROPCS COMMUNICATIONS, INC.

Before the

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
COMMITTEE ON ENERGY & COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

On

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

March 7, 2012

Thank you, Chairman Walden and Ranking Member Eshoo. It is an honor to appear before you and your colleagues on the Communications and Technology Subcommittee today. I hope that you will find my testimony to be informative and helpful as Congress debates the appropriate role of the Federal government in the important area of cybersecurity and private sector communications networks.

My name is John J. Olsen. I am the Senior Vice President and Chief Information Officer for MetroPCS Communications, Inc. I have nearly 30 years of experience in the information technology and communications fields. Prior to joining MetroPCS in April 2006, I served as the Chief Technology Officer at a heath care technology company, as a Vice President of Systems Development and then as a Vice President of Information Technology Engineering at another major wireless and wireline telecommunications provider, and as the Chief Information Officer at a large business network solutions provider. Before that, I held a number of positions managing information technology for a large electric and gas utility. I began my career as a Director of Management Information Systems for the U.S. Air Force School of Aerospace Medicine.

MetroPCS is headquartered in Richardson, Texas, and is a leading provider of unlimited wireless communications services for a flat-rate on a no annual contract basis. We currently are the fifth largest facilities-based wireless provider in the United States based on number of subscribers served, and we operate networks covering approximately 100 million people. As of December 31, 2011, MetroPCS had over 9.3 million subscribers.

As a leading innovator in the wireless industry, MetroPCS was the first provider in the United States to launch a 4G LTE commercial network in 2010, the first to launch a dual mode

4G LTE/CDMA phone and the first carrier to provide a dual mode 4G LTE/CDMA handset using the Android operating system. MetroPCS currently offers consumers 4G LTE services in the following major metropolitan areas: Atlanta, Boston, Dallas-Fort Worth, Detroit, Jacksonville, Las Vegas, Los Angeles, Miami, New York City, Orlando, Philadelphia, Sacramento, San Francisco and Tampa. And with MetroUSA(SM), MetroPCS customers can use their service in areas throughout the United States covering a population of over 280 million people through roaming agreements MetroPCS has reached with other carriers.

MetroPCS also owns and operates approximately 160 retail stores, but the majority of our customers purchase their service plans and phones and pay their bill through thousands of independent MetroPCS dealers, of which a substantial portion are minority or women owned businesses. Consumers also can purchase MetroPCS services through Amazon.com as well as online through our own website.

To support our business and our customers, we use four IT networks for our business and communications network operations. All four networks are critically important to maintaining our ability to provide reliable services to our customers and safeguarding proprietary customer and corporate information. I am responsible for three of the company's IT networks: M-Net, SOA-Net and V-Net. The other network, OD-Net, is operated by our engineering group.

The M-Net (or Metro Net) is used to interconnect our corporate office, regional offices and retail stores. The network carries encrypted subscriber data, email and provides Internet connectivity and data from point-of-sale terminals located in our retail stores. The SOA-Net is the Service Oriented Architecture layer that is mainly used to integrate transactions, including billing, payment processing and customer activations and deactivations, and allows our different

vendors and systems to interact with each other. The SOA-Net resides within the Amdocs data center. The V-Net (or vender net) is the point-to-point vendor network that is mainly used for vender transactions that are not integrated through SOA-Net or which do not interact with the Amdocs billing system. The OD-Net or Operational Data Network is the IT network that connects the facilities and backhaul of our communications network.

All four of MetroPCS' IT networks utilize Multiprotocol Label Switching (MPLS) circuits from two large, well-known and highly reputable national service providers based in the United States. The MetroPCS IT network equipment, including hardware, routers, switches, firewalls, intrusion prevention systems and wireless access points, are made by a major, well-recognized reputable vendor based in the United States.

MetroPCS also operates a separate WiFi network in each of its retail stores for customers and employees to use for demonstrations and other purposes. However, each is a stand-alone private network that does not connect to any of the other MetroPCS networks.

Security of these critical networks and the customer and personal information transmiting over these networks is very important to MetroPCS. To secure these networks, MetroPCS maintains a comprehensive "risk-based" information security program built on industry best practices covering people, process and technology. The foundation for the program includes standards such as COBIT (Control Objectives for Information and Related Technology), ISO 27001 (an international standard for information security management) as well as other compliance-related standards. MetroPCS uses a combination of hardware, software and services to secure its IT networks.

Our security program directives are driven by a formal "governance" function ensuring that the program is aligned based on defined organizational risk tolerance levels. Other program component highlights include centralized policy management, security awareness, training, internal and third-party monitoring, physical protections, threat identification and vulnerability management as well as intrusion prevention.

Further, the ongoing validation and improvement of our security program is based on periodic internal and third-party assessments and auditing.

As for the nuts and bolts of our program, we are especially focused on security at the perimeter and use multi-level security technologies to secure our networks, and to prevent unauthorized access from both inside and outside our company. We also conduct regular network security audits and penetration tests. As part of our security program, we have third party vendors conduct regular network security audits and penetration tests. Further, we have standardized on a single provider for the equipment for all of the networks which, in our view, increases the effectiveness of firewalls and encryption which we use extensively. Our networks are also broken up into segments with firewalls between critical segments. For example, there is a firewall, as well as other security measures, between our retail stores and the rest of our networks. Amdocs, which holds our customers' CPNI, also is firewalled off from the rest of MetroPCS's IT networks. Our independent dealers also do not have access to MetroPCS' IT networks. Rather, they connect through our Amdocs billing system using secure sessions.

For the networks that I manage, we have implemented 24 hour monitoring solutions, which includes devices placed within our network to monitor for any kind of malware, intrusion

attempts or other unusual activity. We also monitor the devices for performance anomalies and suspicious activity which could be evidence of an attack.

Our monitoring efforts, which are augmented by our cybersecurity partners, can generate hundreds of thousands of alerts a day regarding potential cyber threats, but they are pared down through focused review to just a handful of potential threats that merit attention, which we immediately address.

The OD-Net used by our communications network, which is managed by our engineering group, employs similar technology that we use on the other IT networks. It is important to note that MetroPCS has built a 24/7 Network Operations Center ("NOC") in the Dallas area that monitors every switch and cell site on the communications network as well as the OD-Net. The security for the OD-Net is handled through the NOC.

Of course, MetroPCS has implemented numerous physical security measures to protect its data center and NOC, such as the use of multiple levels of card key and biometric access and security. And, MetroPCS has a second data center for disaster recovery in another region of the country where critical systems are replicated to enable the networks and systems to get back up and running in the event of a localized event in Dallas.

MetroPCS' information security staff also maintains vendor-specific and industry-recognized certifications and organizational memberships. In addition, the information security staff regularly participates in vendor-sponsored symposiums and industry summits and conferences. We are involved in these groups not because we are required to, but because they are a valuable source of knowledge sharing and best practices.

While MetroPCS cannot say definitely that we have never had a cyber intrusion, we are not aware of any significant cyber intrusions or cyber attacks that have been successful at disrupting our IT network.

In light of the significant voluntary measures MetroPCS takes to secure its key IT networks without any government mandate and, to date, has avoided any successful cyber attacks, MetroPCS does not believe that additional government regulations are required or warranted at this time, particularly for private sector communications service providers, such as MetroPCS, that do not provide services to the Federal government or local public safety organizations. Private sector companies like MetroPCS are already well incented to protect their networks because their customers would have a negative reaction to cyber intrusion, especially one that disrupts service on the network or exposes CPNI or customer personal information.

This is particularly true for service providers like MetroPCS who provide services on a month to month basis where customers can terminate service at any monthly renewal without any penalty. This provides a powerful economic incentive to protect customer information. Further, there is substantial retail competition for wireless carriers. If MetroPCS does not provide the level of protection its customers want or demand, its customers can terminate service and activate service with the numerous other facilities and non-facilities based competitors. Moreover, wireless providers do have other reasons to voluntarily undertake these measures. Current Federal regulations like the Federal Communications Commission's CPNI rules and private sector certifications such as PCI for credit card transactions also force communications service providers to invest in the appropriate tools and practices to detect and deter cyber threats to their networks.

MetroPCS also believes that private market forces are better suited to respond quickly to constantly changing cyber threats. While MetroPCS does not believe additional government regulation is necessary at this time, if regulations are considered, MetroPCS urges that these commercial requirements be flexible and tailored to the size and amount of threat a particular private sector provider may face. Regulatory compliance can be particularly burdensome for competitors such as MetroPCS who compete by maintaining a low cost structure.

MetroPCS does support the enhanced sharing of information regarding cyber threats by the Federal government as long as there is no mandated reporting requirement imposed on the private sector. Unfortunately, even obligations imposed on industry that start out as "voluntary" could evolve into a burdensome mandatory requirement on industry, where the costs far out weigh the benefits. In that light, a Federal government sponsored central clearinghouse for cyber threats could be useful to private sector entities like MetroPCS and our third party vendors that currently waste a great deal of time tracking false threats. While IT security companies collaborate and maintain their own cyber threat databases, there is no central clearinghouse for industry to utilize. Additionally, MetroPCS supports those who advocate immunity from lawsuits for private sector entities if such a clearinghouse is established. Basically, there should be no liability if a private sector company does or does not use the information that may be available in the central clearinghouse.

Overall, any cybersecurity legislation that Congress may consider should focus more on protecting the government's own critical IT systems and networks from cyber threats and sharing critical information with private industry. And while the private sector may be able to help the government in that regard, it should not be used as a means to impose onerous and unwarranted regulations on the private sector.

Thank you again for the opportunity to testify, and I look forward to any questions that you may have.

Mr. WALDEN. Thank you, Mr. Olsen. We appreciate your comments today and we will back to you with questions as well.

Now we will turn to our final witness on the panel this morning, Mr. Scott Totzke, Senior Vice President, BlackBerry Security Group, Research in Motion, RIM. Thank you for being here and we look forward to your comments.

STATEMENT OF SCOTT TOTZKE

Mr. TOTZKE. Chairman Walden, Ranking Member Eshoo, members of the subcommittee. Thank you very much. My name is Scott Totzke. I am the Senior Vice President of BlackBerry Security at Research in Motion, and I am pleased to be here to talk to you on the topic of cybersecurity.

RIM revolutionized the mobile industry when we introduced the BlackBerry in 1999, and today our products and services are used by millions of customers around the world. There are more than 630 carriers and distribution partners in 175 countries that offer BlackBerry products and services to our customers. More than 90 percent of the Fortune 500 customers are BlackBerry customers today, and we have a longstanding relationship with the U.S. Federal Government including Congress, the Department of Defense and the Department of Homeland Security.

Mobile communications face similar security risks as non-mobile communications. Several of the same types of threats and attacks that have existed in traditional computing platforms can impact smart users today, and as the power, ubiquity and computing capabilities of smartphones have increased over the last few years, the threat matrix continues to evolve exponentially. Most users have yet to realize the applicability of both the existing and emerging threats to what is essentially a smaller and more mobile computing platform that they already have at their home or office.

An effective and comprehensive mobile security solution must therefore provide protection by proventing unauthorized access to the smartphone and its data, to protect the data in transit over the wireless network and to protect the corporate network using features that are built into the platform. While technology vendors can provide components of these solutions, it is equally important that as a mobile technology industry, we help government, enterprises and consumers better understand the risks involved with all types of online activities.

For our part, RIM focuses on designing secure and efficient solutions for enterprises and consumers. RIM has a history of integrating security features into its products and firmly believes that security technologies are an important foundation for a digital economy. RIM has built security features in that allow for data to be encrypted and protected from unauthorized access, to limit and control access to information on the smartphone by third-party applications, and to remotely erase sensitive information in a case where a phone is lost or stolen. These controls can all be centrally managed by the BlackBerry Enterprise Solution, which is designed to give large and small organizations the ability to balance individual and enterprise use of BlackBerry smartphones while protecting the privacy of their corporate and employee information.

RIM also believes that there needs to be more focus on security testing and certification that establishes a baseline for technology vendors. Without an established baseline to properly gauge the security of a product or a network, it is difficult to make informed decisions. Vendors that work to certify their mobile solutions through trusted validation programs provide assurances to governments and consumers who would otherwise be unable to verify the security of the claims being made by the vendor.

BlackBerry products and solutions have already received more security accreditations globally than any other wireless solutions, and our consumers value this level of transparency when it comes to protecting their information. We feel that greater adherence to security standards like FIPS would help customers better understand their personal and professional investments in protecting their information.

Lastly, this panel has raised a number of concerns regarding two extremely important points related to the evolution of security and technology in the mobile industry that I would like to address. The first concern is related to information sharing. While there is increased competition between vendors, there is also an increasing degree of commonality in the components used by many desktop and mobile platforms. This directly translates into an evolving risk of cross-platform vulnerabilities, creating a level of shared risk that increases the need for vendors to work together to responsively disclose and address these concerns. This also means that programs such as RIM's information sharing program need to fully engage with public sector entities such as the US–CERT to ensure timely and bidirectional flow of security information.

The second issue raised here is related to supply chain security and the impact it can have on the security and availability of networks. A product that has been modified or created in an authorized manner could pose security risks to the customer's information and to the overall posture of RIM's network, our carriers' networks or our customers' networks. RIM has been working for several years to embed network security elements directly into the silicon of our products and in all aspects of our manufacturing process to ensure that only authentic products are allowed to obtain network services. We believe that this combination of hardware security, operational security and manufacturing, facility security, software security, network security work together to mitigate many of the concerns about knockoff products or products that have otherwise been tampered with, impacting the security of our customers' information. We support the subcommittee's efforts to raise awareness of this wide-reaching impact in respect to supply chain-related security issues.

Chairman Walden and members of the subcommittee, I would like to thank you again for the opportunity to provide RIM's perspective on these critical issues.

[The prepared statement of Mr. Totzke follows:]

Statement of Scott Totzke

Senior Vice President, BlackBerry Security Group

Research In Motion

before the

Subcommittee on Communications and Technology of

the House Committee on Energy and Commerce

on

"Cybersecurity: The Pivotal Role of Communications Networks"

March 7, 2012

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, my name is Scott Totzke and I am the Senior Vice President of BlackBerry Security at Research In Motion. I am pleased to appear before you today to speak on the issue of cybersecurity.

Research In Motion (RIM), a global leader in wireless innovation, revolutionized the mobile industry with the introduction of the BlackBerry® solution in 1999. Today, BlackBerry products and services are used by millions of customers around the world to stay connected to the people and content that matter most throughout their day. Founded in 1984 and based in Waterloo, Ontario, RIM operates globally in the Americas, Europe, the Middle East, Africa and Asia-Pacific. There are more than 630 carriers and distribution partners offering BlackBerry products and services in over 175 countries around the world. More than 90% of the Fortune 500, as well as countless government agencies, are among our customers. We have a longstanding relationship with the federal government. RIM is proud to serve the U.S. Congress,

the Department of Defense, and the Department of Homeland Security, just to name a few of our valued federal customers.

Mobile communications face similar security risks as non-mobile communications. Several of the same types of threats and attack techniques that have existed on traditional computing platforms can impact smartphone users as the power, ubiquity, and computing capabilities of smartphones have increased over the last few years. Most users have yet to realize the applicability of both existing and emerging threats to what is essentially just a smaller and more mobile computing platform than they already use in their home or office.

As with any computer security solution, a mobile solution must take into consideration what applications the smartphone will need to run, what data it will need to send, receive, and store as well as the regulations with which the organization must comply. While the challenges and security concerns are constant regardless of whether the computer is mobile, mobility requires additional considerations due to the constraints of the platform relative to a desktop PC (in terms of screen size, computing power, battery life, and network capacity) and the ubiquity of mobile smartphone use across diverse populations. An effective and comprehensive mobile security solution must therefore provide protection by preventing unauthorized access to the smartphone and its data, to data in transit over the wireless network, and to the corporate network using features that are built into the platform in order to properly account for these inherent limitations. While technology vendors can provide components of these solutions, it is equally important that, as a mobile technology industry, we help government, enterprises, and consumers understand the risks involved with all types of online activities.

The topic of cybersecurity is becoming increasingly predominant in discussions related to the worldwide growth of mobile data and communications for consumers and enterprises. At its core, cybersecurity means protecting and securing our networks from all forms of attacks and ensuring that these networks continue to operate in times of crisis. For governments and enterprises this is best done through the application of a cybersecurity policy that enhances the safety of an organization, its partners, and its customers, thereby minimizing the risk of exposure and possible exploitation and maintaining valuable brand credibility. The cumulative measures

that individuals and organizations take to protect their network assets (personal computers, mobile phones, servers, and so on) are generally known as cyber defense. To understand the impact of cybersecurity and cyber defense in the global conversation, and most relevant to this Subcommittee, we must understand the value of security in mobile communications.

RIM focuses on designing secure and efficient solutions for enterprises and consumers. A longtime innovator and leader in mobile communications, RIM has a history of integrating security features into its products and firmly believes that security technologies are an important foundation for a digital economy. Furthermore, RIM's position is that built-in security features are essential to the delivery of any technology that will be used for mobile communications if governments, enterprises, and citizens are to benefit from a consistent foundation of security. RIM has also built in features that allow for data to be encrypted and protected from unauthorized access, to limit and control access to information on the smartphone by third party applications and to remotely erase sensitive information in the case where a smartphone is lost or stolen. These controls can all be centrally managed by the BlackBerry Enterprise Solution, which is designed to give large and small organizations the ability to balance individual and enterprise use of BlackBerry smartphones while protecting the privacy of their corporate and employee information.

Without this level of built-in security, individuals and organizations are left to employ a variety of solutions, including antivirus software, firewalls, and encryption, to help protect personal information on mobile platforms. As an industry, we need to meet the public demand for secure personal and business information, and our communication solutions need to provide built-in security features that allow users to manage their privacy protection easily and consciously. Every security decision is an exercise in risk management and we need to ensure that the technology that users have access to provides a level of transparency and assurance around the protections afforded to them by their mobile solution providers.

RIM also believes that there needs to be more focus on security testing and certification that establishes a baseline for technology vendors. Security is a complex discipline that requires users to make informed decisions about their information. Without an established baseline to

properly gauge the security of a product or network, it is becoming increasingly difficult to make these informed decisions. Vendors that work to certify their mobile solutions through trusted validation programs provide assurance to governments and consumers who would otherwise be unable to verify the security of the mobile technologies they use. BlackBerry products and solutions have already received more security accreditations globally than any other wireless solution and our customers value this level of transparency when it comes to protecting their information. Greater adherence to security standards like FIPS would help customers better understand their personal and professional investments in protecting their information. The assurance that the information of a business, however large or small, established or entrepreneurial, is trusted and suitable for use by some of the most security-conscious organizations in the world is an essential cornerstone in developing trust and confidence in the online economy and its established and emerging brands. As citizens merge their private and business lives on their mobile smartphones, this principle becomes essential to their safety and livelihood.

RIM owns and operates the global BlackBerry Infrastructure (sometimes referred to as the Network Operations Center or NOC) and manages the delivery of wireless messages on various wireless networks sent to and from BlackBerry smartphones. This model simplifies wireless for customers and optimizes protocols for wireless environments by creating a trusted bridge between private networks – the customer's internal network, multiple carrier networks, and RIM's service delivery infrastructure — yet it also ensures that there is a trusted path between all parties that is based on strong, cryptographic, mutual authentication.

The BlackBerry Infrastructure is an integral part of RIM's ability to deliver industry leading push services, security, manageability, and spectral efficiency for RIM's customers and partners. It is designed to efficiently manage the transport of messages between the wireless network and a smartphone and it transfers more than 25 petabytes of data traffic in a month. All messages sent to and from BlackBerry smartphones can be routed through the BlackBerry Infrastructure by default and the BlackBerry Infrastructure is designed to provide a highly secure connection between an organization's network and its smartphones.

Unlike traditional VPN solutions, the BlackBerry solution utilizes built-in, efficient protocols that allow them to authenticate with each other while they transfer data. By building mutual authentication and security directly into the data transfer protocols, the system ensures that every packet contains information that is useful to the end user. This is especially relevant in times of crisis when carriers' network infrastructure can become overwhelmed or are operating at a greatly reduced capacity. The blend of security and spectral efficiency allows BlackBerry smartphone messaging systems to remain fully operational when most in need – an essential element of any mission critical network.

Lastly, the panel has raised concerns regarding two extremely important points related to the evolution of security in the technology and mobility industry that I would like to address.

The first concern is related to information sharing. While there is increased competition between vendors there is also increasing commonality in the components used by many desktop and mobile platforms. This directly translates into an evolving risk of cross platform vulnerabilities, creating a level of shared risk that increases the need for vendors to work together to responsibly disclose and address these concerns. This also means that programs such as RIM's Information Sharing Program (RISP) need to fully engage with public sector groups such as US CERT to ensure the timely and bidirectional flow of critical security information.

The second issue raised is related to supply chain security and the impact it can have on the security and availability of networks. A product that has been modified or created in an unauthorized manner could pose significant risk to the security of our customers' information and to the overall security posture of RIM's BlackBerry Infrastructure, our carrier partner networks, or our customers' networks. RIM has been working for several years to embed network security elements directly into the silicon of our products and into all aspects of our manufacturing processes to ensure that only authentic BlackBerry products are allowed to obtain network services. We believe that this combination of hardware security, operational security in manufacturing facilities, software security, and network security work together to mitigate many of the concerns about "knock off" products or products that have otherwise been tampered with.

We support the Subcommittee's efforts to raise awareness of the wide-reaching impacts of the supply chain security issue.

Chairman Walden and members of the Subcommittee, I would like to thank you once again for the opportunity to provide RIM's perspective on these critical issues.

Mr. WALDEN. Mr. Totzke, thank you very much for your testimony. All of you, thank you very much. We appreciate your being here.

I am going to lead off with questions. So Dr. Amoroso and Mr. Olsen, you say in your testimony that you routinely track threats to your networks. I assume you all do that. How can we facilitate information sharing among network providers of such information while protecting consumers' privacy and companies' competitively sensitive data?

Mr. AMOROSO. I think the big debate has been between government and industry, right, that has been the big issue. Like if I go to a security conference and some hacker whispers to me that there is a signature that I should be looking at, then I scribble it down, run back to my op center and put it in place. If a government individual does that, then I can't put that in the network because we would be operating as a branch or an agent of the government or something like that. So that seems to me a little silly, like that is something that probably ought to be addressed.

Mr. WALDEN. That is the kind of specific issue we are trying to drill down to here. Can you give us something more specific? Where does that show up? Do you know statutorily?

Mr. AMOROSO. Oh, yes. I mean, like the United States intelligence agencies and law enforcement agencies regularly see different types of signatures that we don't look for. We are not in law enforcement. We are providing service to customers. We don't chase that sort of thing down. We chase it to the point where we can stop it, and that is it, but like intelligence groups will really dig down deep and see something that we don't. For them to share that, particularly if it is classified or something is awkward and it is stilted. And I know in my own company whenever I get involved in something like that, there is more lawyers involved in the discussion than there are people in this room right now. So, you know, it is almost like we are disincented to even bother. So I don't think it is so much whether, you know, between different groups we share because, frankly, we kind of do. The Internet wouldn't work if we weren't sharing constantly.

Mr. WALDEN. But are there any prohibitions? If you spot something, if you go to that conference and a hacker says look for this signature, is that something that Mr. Olsen, Mr. Mahon and others should be looking for as well on their networks?

Mr. AMOROSO. I am sure they do.

Mr. WALDEN. And then is there a way you can share that information with them or are there impediments to that kind of sharing?

Mr. AMOROSO. I mean, we all buy services from a lot of the same companies that do that. You know, we pick companies that do a really great job of that. I buy from three or four different companies that provide about the same intelligence everybody else is going to get. You know, it is pretty good, you know, and they are incented to make sure it is pretty useful because I pay them every month for it.

Mr. WALDEN. And do the customers. And so I guess the question then is, there is not a problem sharing information back and forth?

Mr. AMOROSO. Sometimes there is, right?

Mr. WALDEN. Is that a problem we should address? We are looking for barriers.

Mr. AMOROSO. I mean, here is the classic example. AT&T had an exclusive on the iPhone for some period of time, so I put a bunch of people down in New York City, PhDs right out of school and I told them find ways to filter attacks being aimed at iPhones, that will really help our customers, and they worked real hard and we came up with some, and once other carriers got access to the iPhone, do you really think I would want to give them, you know, the fruits of the work that we are doing? Their incentive is to do it as well and, you know, compete with us, and I would like my customers to say hey, I am going to stay with AT&T because they are really investing in doing protection and our competitors say the same thing, and we innovate that way. That is kind of—that is a case where, you know, it is not necessary for me to share. The market is going to force our competitors to want to catch up or for me to catch up to somebody else. That is the right balance between, I believe, all of us. But between government and industry, I think the information sharing should be more free.

Mr. WALDEN. Thank you, Doctor.

Mr. Olsen, do you want to comment on that?

Mr. OLSEN. Thank you, Mr. Chairman. At MetroPCS, besides our internal controls and our internal systems, we also have cybersecurity partners, so securing monitoring firms that we use to monitor our network and our systems 24 hours a day. Those firms do share information between them, but if I believe I understand your question, there is not a central clearinghouse for that information for the folks that are outside of those security companies to easily share information. So if Mr. Amoroso recognizes a threat or is told about a threat in his network, there isn't a central place where he could notify other companies or other carriers even in the same industry that this threat is out there and we should respond to it.

Mr. WALDEN. And is there an incentive? Because I almost a disincentive to do that. If you have done the research, you identify the threat, you protect your customers, why do you tell other iPhone——

Mr. AMOROSO. I don't know that it is a disincentive. Keep in mind that when we advertise or broadcast that there is a threat we are worried about, you are telling the bad guys too, right? I mean, so it is a little—it would be a little weird to be too open about what you are concerned with. So I kind of like the existing model. I mean, I think that there are companies that do this. We evaluate them, and when the intelligence looks pretty good, we buy it.

Mr. WALDEN. All right. My time is expired.

We will turn now to the gentlelady from California, Ms Eshoo.

Ms. ESHOO. Thank you to all of the witnesses. Excellent testimony.

First to Mr. Livingood, I think it is really terrific that you are the first ISP in North America to fully implement the DNSSEC as you noted in your testimony. How do we encourage other ISPs to follow your lead? What would be—just quickly. I have a whole series of questions.

Mr. LIVINGOOD. So I think on that question regarding DNSSEC adoption by other providers, I think it is important to keep in mind one thing, which is, it is not just about network operators, it is about banking sites, it is about other Web sites, software developers. A lot of people have to implement DNSSEC to make it work in the ecosystem. But specific to network operators, I would say that there is actually already a lot of that interaction going on already. You know, one of the beautiful things about the way that the Internet has worked and is successful is, there is a lot of these multi-stakeholder consensus-based organizations that groups get involved in. One of them in fact happens to be one of the CSRIC working groups that I am on, and they will be coming out with a recommendation soon, and a number of our companies participate——

Ms. ESHOO. When will that be?

Mr. LIVINGOOD. I think that it is due today, the recommendations.

Ms. ESHOO. Oh, good. You never know on government time. Congress has an extensive network to ensure the security of our mobile devices and the network that they run on. I experienced this firsthand last year when I traveled abroad as part of a Congressional delegation, and my device became infected during the trip, and the device never left me. I mean, I practically slept with the thing under my pillow. It never was out of my purse. It was never left in the hotel. But nonetheless it was infected. The good news is, because of the proactive measures in place, the threat was detected prior to being reactivated in the House network. So as a company, what steps do you take to ensure that your customers, particularly those in smaller organizations, adhere to the same proactive security measures? And I guess my question is to Mr. Totzke, to Dr. Amoroso—I love your name, Amoroso—and Mr. Olsen.

Mr. TOTZKE. Thank you, Congresswoman. I will go first. I mean, we provide a comprehensive list of guidelines for configuration of the device so our administrators have white papers and information they can access on the Web site, and our goal is to make sure that your administrator, your IT organization that looks after your device if it is a BlackBerry device has full control over that device at all times, so there is a comprehensive set of policies, more than 500 of them, that an administrator can send to control all aspects of the platform including preventing access to information or disallowing you the installation of software on the device. So we try and do that. As I think will be a common thread here, there is a lot of education in this industry. Security is a complex set of decision-making things that we have to do on a daily basis and a lot of risk that is really difficult for people to understand. We are trying to offer as much transparency and help to our customers through publication of standards and best practices and forums like this.

Ms. ESHOO. As I understand, one way to prevent potential botnet activity is to isolate and block IP addresses that pose a threat. Do you all have the technology to do this today, and if so, has it been effective?

Mr. AMOROSO. I can comment. I mean, we have the technology to block but it doesn't work, so, you know, we can certainly—we do

try. We try real hard. Botnets all of your PCs being infected. That is what it is. Like we have made the mistake in computing of turning every person in this room into a Windows system administrator. That is what you do part time when you are not legislating. So that model is wrong, and most of you don't do a very good job of it, nor do I. I bet people at this table, we would shrug and say we probably don't do it well either. So we have distributed the responsibility massively and that risk——

Ms. ESHOO. Is that what causes the complexity that you just discussed?

Mr. AMOROSO. Well, it is billions of people around planet Earth with PCs that are improperly protected, so it is a piece of cake to build a botnet. We watch botnets, you know, new ones every day, ones that are 50,000, 100,000 botnets we don't even bother naming. We just say oh, there is another one. We track them and just try to contain it. So it is not a matter of blocking the IP addresses, because we would be blocking you. You probably wouldn't like that. "Sorry, you can't get on the Internet today. Why? It looks like you have a botnet." We would just shut the whole Internet down if we did that.

Ms. ESHOO. In my opening statement, I mentioned the issue of supply chain and the security that I think really needs to be brought to that. First of all, do you share these concerns about the supply chain, and if so, what do you think would be the appropriate role for us to play in addressing it? I think it is a serious issue. Our telecommunications network that we came to more fully appreciate after our country was attacked was the system that we relied on. If we didn't have that, I don't know what we would have done. So I think that—and there are constant things that keep coming up relative to the supply chain. So I welcome any comments on that.

Mr. TOTZKE. So I will answer that from a device manufacturer's standpoint. You know, this has been a concern for RIM for the decade-plus that I have been there. We have to understand where we get our components from, where we manufacture the devices, and when we started, it was real easy because we just made everything in our factory and it was all under our control and you grow into a global entity, you deal with outsourced manufacturing and kind of distributing that capability around the world with different partners. So it brings into question, you know, are you actually manufacturing the product you think you are making or are you getting something that is whole and intact. We have really focused on understanding what we can do to secure our products in the manufacturing process as well as the parts that come in. So for some of our strategic vendors, we are actually doing serialization and embedding kind of cryptographic elements in their silicon before it gets to us, and then our manufacturing process goes through a verification of every tool along the line, checking with RIM head office to say are you allowed to actually perform this operation, and the combination of hardware and software, so the embedded certificate is in the silicon. The hardware checking that the software hasn't been tampered with is used to authenticate the device to get BlackBerry services. So we know that a device hasn't been tampered with and it has been manufactured by RIM and it is intact

when you first turn it on, and that authentication protects our network, our carrier partners' network and your networks, and is that hardware, software and network layer all working together to ensure the integrity of the BlackBerry services that we provide to our customers.

Ms. ESHOO. Thank you.

Mr. WALDEN. Thank you.

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

Mr. TERRY. Thank you, and with my 5 minutes and five people, I want to ask you all the same question, and that is in regard to the fact that you are the interface. If I want to have an Internet experience, I have to hire one of you. So what are you doing to provide me services that will protect at least to some extent from botnets and viruses or attacks to my information and my computer? And we will start from left to right, my left to right, Mr. Livingood.

Mr. LIVINGOOD. Sure. Thank you. So I think we all have somewhat similar, you know, capabilities. It is a multilayered approach. There is not any one thing that is going to solve it. So it is sort of, you know, like an onion. There is lots of layers, and it is everything from intrusion protection that is at the edge of a network to things that provide denial-of-service attack, you know, mitigation when you see those things to botnet intelligence systems that detect botnets and start to notify customers—I mentioned that in my opening statement—and then to notify customers, and there are also a number of things that we all do and we do in particular to educate customers, to help them understand what things they need to secure in their network, the software they need to manage, gets them the software that they need to secure their network and their computers. So it is a multilayered approach.

Mr. TERRY. Mr. Amoroso?

Mr. AMOROSO. That was exactly what we do, same thing. There are a lot of different products and product names. I mean, I will tell you the one thing we don't do, and that is, we didn't sell you the computer, we didn't sell you the operating system that runs on the computer and we didn't help you select what type of software to put on there, and increasingly the ISPs are getting dragged into that, and it is a difficult situation because, you know, a lot of times people will say ISP, you know, I got something wrong with my PCs, you guys are sitting off in a cloud somewhere watching, you should figure out how to fix my PC, and that is something all of us struggle with.

Mr. MAHON. We do all a number of very similar things, I think, in the ISP world, you know, to protect particularly residential customers. I think you have heard the spyware, the anti-virus, parental controls. We all have education and awareness, you know, places on our Web site, our home page where you can go to. We have a botnet notification program. In fact, if your computer does become a bot on a botnet, we have a method to notify you and then facilitate you cleaning up your home device.

Mr. TERRY. Mr. Olsen?

Mr. OLSEN. I think there is a lot of commonality in the approaches that we are all taking. One of the distinctions that I made

in my opening comments regarding our cybersecurity partners I think is really important. These are people that are focused, that their full-time job is cybersecurity. They are looking for threats all the time and they have hundreds, if not thousands, of customers that are feeding them information and they are seeing real-time threats go through many companies. So a threat that might hit one company, they are aware of before many of us would see that. So I think that information sharing in that cybersecurity industry is really critical and it is something that we value.

Mr. TERRY. All right. Mr. Totzke, you may have already answered this question when you were talking to Ms. Eshoo.

Mr. TOTZKE. Yes. So certainly the embedded security elements are part of that but beyond that, you know, we have user- and administrator-controlled security that lets our users dictate what level of protection they want to put into the platform, and we do have services available to consumers and enterprises that allow for on-device encryption of data, remote backup, remote restore, the ability to remotely lock and wipe the device so you can deal with this eventuality as a mobile device that is going to be lost or stolen or left in a taxicab, so we give you the capability out of the box to deal with any of those eventualities.

Mr. TERRY. Good. I appreciate that. I guess the last 47 seconds I am going to give to Mr. Amoroso. Should the responsibility be on the ISP providers to have a system to detect viruses as they enter into your network before they get to my computer?

Mr. AMOROSO. If we knew how to do that reliably, I would have been trying to sell you that years ago. It is a very difficult thing to detect viruses and malware. Sometimes we can kind of pick it up, and we do notify, just like the rest of them. I call 100 to 1,000 people very week. The problem is, if I really knew what to tell them, knew exactly how to fix their PC, I would call everybody. Why just restrict it to the ones that happen to notice active malware? We would tell everyone. The problem is, there isn't a person in this room that can tell you how to clean malware off your PC other than reimage your computer. You know, that is the best we can do.

Mr. TERRY. Can't we just tell you to stop it?

Mr. AMOROSO. I wish I knew what—you know, here is the reason we can't stop it. I don't know if you are familiar with the concept of an encrypted tunnel, but when you visit a Web site and see https, that means there is cryptography between you and the Web site and everybody says oh, that is really secure, you should look for that. The reality is, every hacker in the world knows to make sure they are pushing their malware through that encrypted tunnel because none of us can see it. So we can sort of block the Web site but they hide the malware in places we can't see. That is where anybody would go.

Mr. TERRY. Well, it is such a fun issue to deal with.

Mr. AMOROSO. Here is what—when we pick up malware, it is the equivalent to somebody falling over and having a heart attack on the table, and we all go, that is rapid response to preventive care. You fell over, you had a heart attack, I picked that up. That is easy. It is picking up the stuff that isn't easy, and that is why it

is difficult for us to build reliable services that will detect malware because it is hidden. Any hacker would do it that way.

Mr. WALDEN. Thanks.

Mr. Doyle, you are up next.

Mr. DOYLE. I think we ought to just call him Dr. Sunshine.

Mr. Totzke, I want to ask you about Federal workers. As you might know, the White House is currently working on a national mobility strategy to determine how the employees of the Federal Government are using their mobile devices, and they are going to decide, for example, whether all agencies can bring their own devices to work much like many private sector employees do. Now, we don't of course advocate to prescribe one particular type of phone for everyone to use in the Federal Government but what security issues do you foresee that might come up as a result of this if we allow all Federal workers to use their own mobile devices and how do you think device manufacturers can make sure that the data that is on the phone of Federal workers, especially in sensitive agencies, remains secure?

Mr. TOTZKE. So as you move to more of a heterogeneous environment where you bring your own device for what we call personal liable, individual liable devices, one of the challenges you face is that the security of platforms is going to vary based on the vendor and the posture and the features that they built into that. So getting a consistent view of security and how you are protecting your information is probably one of the issues. There are, you know, kind of liability and discovery issues in more of a corporate context—who owns the information, who owns the intellectual property if you have to go through any kind of a litigation, maybe not so much in the case of a Federal Government employee, and then how do you protect the information on the device, which I think is probably one of the more important ones. You know, there is a level of encryption built into BlackBerry to encrypt all of that data at rest, whether that is personal data or government data, and that is one of those that can be enforced remotely. But as we look at how we go into a bring-your-own device scenario, you know, the biggest concern that I have is this lack of a standard bar for protecting information, and what I would be most concerned about is sort of a race to the lowest common denominator so we have three or four competing platforms, so in order to allow everything we are going to reduce our security requirements to the bare minimum, which I think is the wrong thing, especially at the government level.

Mr. DOYLE. Thank you.

Mr. Livingood, given the concerns outlined by Dr. Sunshine about implementing the DNSSEC, can you outline for us why Comcast made the decision to begin using DNSSEC and whether you think it has had the intended benefits that you hoped it would have?

Mr. LIVINGOOD. Sure. Well, you know, the intended benefits, it is a long-term game there. I think one of the challenges with DNSSEC adoption was that you needed some critical mass for people to start signing their names, for people to build software to do that, and we felt like we could play a role in leading the industry in creating that critical mass. So, you know, that is part of the rea-

son that we did it. I think the reason, you know, at root why we did that is, when the Kaminsky vulnerability came out in 2008, it fundamentally scared the heck of us. If our customers couldn't be sure that when they went to BankofAmerica.com it was that Web site, that scared us because then, you know, they are less likely to use the Internet, they are not going to care as much about higher-speed services and so on, and that is incredibly important to us. So to have a way—we all certainly had a short-term fix to that but to have a long-term fix to that we thought was incredibly important, and DNSSEC appears to be that one, and we are pleased to help lead the way and create that critical mass to help adoption.

Mr. DOYLE. Thank you.

And just in closing, Dr. Amoroso, I have enjoyed your testimony and it makes us all realize how much work we all have to do together to face this problem that certainly there is no easy answer to. But I want to thank all the panelists for your testimony today. It has been very enlightening.

I will yield back, Mr. Chairman.

Mr. WALDEN. Mr. Doyle, thank you very much, and we will go now to Mr. Shimkus for 5 minutes.

Mr. SHIMKUS. Thank you.

I kind of want to build a little bit on what my friend Mike Doyle mentioned, but I want a different perspective, because it popped in my mind when he talked about Federal workers. Where are you finding your cyber warriors today from? In other words, where are they coming out of? Are they coming from private universities? Are they coming out of the military? Briefly, the cutting-edge new people who are helping you do this stuff, where are they coming from?

Mr. LIVINGOOD. So I will start. I think it is a variety of places, and I would say, you know, there is a need for more educational focus not just in cybersecurity but ICT generally, but we find people in a variety of ways. Some are former military service members, former law enforcement. Others are just Linux system administrators that are interested in security. Others are, you know, former childhood hackers or something like this, and they are interested in it. So it is a variety of things.

Mr. SHIMKUS. But is there a college path? I mean, can you get IT training in the business schools or computer science classes?

Mr. AMOROSO. I would like to comment. So I have been teaching at Stevens for 22 years. I teach this semester. If you looked at my class in 1990, you would see something that would look like a typical college class. I went to Dickinson, Pennsylvania, so pretty—a mix of kids. My class today at Stevens is about 98 percent foreign nationals, and I have got about 65 in the classroom, and almost all of them have the intention of leaving the country when they complete their master's or PhD because they see bigger opportunities elsewhere.

Mr. SHIMKUS. Well, and that kind of segues, and if you all want to jump in, you can real quick, but I don't want to forget the aspect of compensation for people entering the private sector versus the government sector. There is this debate on salary compensation. I don't know where it is. I mean, we have the same issues about bringing in the best and the brightest, but if we are not compen-

sating them for what the private market bears, then there is another thing. Does anyone want to jump in?

Mr. TOTZKE. Just on where we source. So there is certainly out of the education system, out of the military and intelligence, we find some people kind of moving into private industry. The most talented guy on my team is a high school dropout, and so I think using the education system as a bar doesn't really help identify the best talent. He would be one of the top recognized kind of hackers and researchers in the world. So it varies, and I don't think you can actually teach somebody to be a hacker. There is sort of if you want to be a researcher in that area, there is an ingrained mentality you are either born with or not, so it is not like I am teaching somebody a trade like programming and getting to a level of sophistication in developing software. Being an attacker is a much different mindset.

Mr. SHIMKUS. Right. Thanks.

You know, the debate on the Senate side, and this is how you provide is, what happens if the Federal Government requires you to follow a new government security standard? What happens to you? That is the debate on the Senate side legislatively. One has a government-imposed standard. One is really, I think, letting you guys fight the battle yourselves. So does anyone want to jump in?

Mr. AMOROSO. I will offer just a brief point. My guess is, anything you can write down that you can think of as kind of a best practice is already being done here, and the things that we are back at the shop worrying about now are things that are not on your list, like as an example, we talked about botnets. You know when I saw the first botnet? Remember Y2K? We were building the Y2K White House communications fusion center, and we were worried that we were going to get DDoS'd for one day. That would be really bad if you are knocked out one day and miss the millennium change. You can't really move that date, right? So we were completely freaked out by botnets then and we have built—a lot of people in this room, we have built ways to steer traffic around and fix it and now we have a service and we moved on to the next thing.

Mr. SHIMKUS. Yes, and let me put a final challenge out because I do agree, how do we incent innovation in this area, which is part of the opening statements. Incentivizing usually means government money here or government tax credits. You know, that is all kind of persona non grata right now in this new world in which we live in, so I would ask you to help us wrap around about this, and maybe it is easing regulatory burdens. Maybe there are things we can do that are not a dollar-cents component but tax credits, things like that. It is very difficult to do in today's environment. I will just throw that out.

Thank you, Mr. Chairman. I yield back.

Mr. WALDEN. I thank the gentleman.

And with the committee's indulgence, Doctor, could you just explain DDoS?

Mr. AMOROSO. I am sorry. That stands for distributed denial of service. Here is how it works. When my voice talks to all of your ears, it is one thing to many ears and it works great if you are all quiet and you listen, your ears work. But if you could bounce my voice off your ears to him, it would sound like you are all shouting

at him, right? My voice to all of your ears and then you reflect it back, that is a denial-of-service attack. We hit all your PCs and then tell all your PCs to shout this way, and boom, it all comes and it sounds like this big attack and it clogs the pipes and knocks them out. That is how it works.

Mr. WALDEN. All right. Thank you, Doctor.

Now we go to Ms. Matsui.

Ms. MATSUI. Thank you, Mr. Chairman, and this is all challenging and frightening at the same time here, and I do appreciate all of your testimony.

I want to go into another area here. As we look into developing industry best practices standards for ISPs, should ISPs' own cloud services be included as well as other cloud providers or do you think because that technology is newer, it could be better for cloud providers to consider forming their own best practices to secure data in the cloud? I would like Mr. Mahon and Dr. Amoroso to answer that, please.

Mr. MAHON. Well, first of all, we are already talking to the cloud providers, and some of us in fact are cloud providers. So I do think that the conversation is well underway. We are very familiar with the challenges, and if you really think about it, the term "cloud" is a rather generic term that is probably misunderstood. It can mean a number of different things for a different type of customer, and so therefore I would say we continue to include them in the conversation as we have everyone else, so to speak, at the table as partners and the solutions that you are looking for are really going to have to be integrated across a very wide platform. So therefore I would say that you would want to keep them in the conversation.

Ms. MATSUI. OK. Thank you.

Mr. AMOROSO. So my mother has a PC at home that at this instant I am sure is like attacking China or something. It is not administered properly and she has got, you know, a big tower with Verizon FIOS, the whole thing. She doesn't need that. She would be better much served to have a cloud provider just take care of all of that for her, and she should just be using, you know, some appliance to hit the Internet. The reason she doesn't is because there is software on the PC that she wants to be able to use that hasn't been put in the cloud. So in general that concept is a more secure concept than my mom trying to do it administration. So I think cloud in general is a more secure model than the one we have now.

Ms. MATSUI. Oh, OK. That is good to know.

Dr. Amoroso, given your expertise in this area, what are the differences between securing wired and wireless communications networks and how can these differences be accounted for in any type of cybersecurity initiatives?

Mr. AMOROSO. Well, they are pretty big, right? The differences are significant. You know, if we had 3 hours, I could take you through the whole thing, but I will give you one example. Remember when—I am guessing most of you remember when computer security was just don't put an infected floppy in your computer. Remember that?

Ms. MATSUI. Yes.

Mr. AMOROSO. And it was like don't put software on your machine that you don't know where it came from. It seemed like perfectly good common sense, right? What do we do every single day on app stores? You know, we are downloading stuff, I don't know who wrote that, I don't know where it came from but boy, it sure looks pretty cool, I think I will download it to my device. That is something we are going to have to address from a security perspective. That is the big difference between wired and wireline.

Ms. MATSUI. OK. I am also thinking that so much of what we do is wireless, so much we do within our homes is wireless, and yet it is just so easy to do it that most people don't think about it at all, and I am concerned that we are not thinking as broadly as we should be thinking as far as some of the personal use, and I think it came about here with Mr. Doyle's too and the government area too. But it is so easy to be carrying tablets and different cell phones around, and for me, the part that is really to me quite frightening is that nobody knows what they don't know, and we are looking at you and you are saying too that there is a lot of things you don't know too, and we look upon you as experts, and I am hoping that we can build in some incentives here with sort of a sharing of information that goes beyond some of your commercial type of concerns. Because I am looking ahead, this is even getting more and more complicated as we develop more tablets and smartphones and whatever that we are losing control of the cybersecurity aspect of it, and the software aspect, I think you brought up, Dr. Amoroso, is really important, the education facet of that, and actually kind of building our principles and standards into that too.

So that is just a comment, and I really do appreciate your being here, and I think I am learning more and more every time one of you opens your mouth, so thank you very much for being here.

Mr. WALDEN. Thank you for your comments.

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

Mrs. BLACKBURN. Thank you all so much, and I tell you what I think I am going to do is just ask my question, then if you all want to respond or respond in writing, that would be wonderful.

First of all, going back to something that Mr. Shimkus said, I would like to hear from each of you, and you can say it now or send it to me, what you are seeing as the disturbing trends and what is kind of the next thing out there. I would like to know that. I would like to get an idea of how much of your cost of doing business is beginning to center around the cybersecurity issues.

In your testimony, several of you have mentioned in one way or another either in response to the questions or testimony fear that the Federal Government could end up being more of an impediment than a facilitator in bolstering some of the cybersecurity efforts. I would like for you to speak to what you are concerned that we might do and then what we are not doing that we should be doing and hear from you in that vein with your consumers, I would appreciate knowing what you are doing to educate them. I think that one of the things that helps us as we work through the process is being certain that consumers are educated, so if I could get that bit of information.

And then when we look at the hacker attacks that are out there, some of the anonymous attacks, some of those, there is one in the news today, I think there are five people that they are bringing forward on charges. What kind of government-imposed performance requirements would help keep pace with some of the technological evolution that you are seeing in these cyber attacks? And if we were to do a government top-down sort of structure to try to deal with cyber enemies, would that be giving a signal to that cyber enemies? Is that kind of too much information for them to be able to work around?

So those are the questions that I would love to hear from you on—the trends, the costs, what we are doing, what we are not doing, dealing with consumers, how you are educating them and then looking at the attacks, the cautions you would give to us there, and with that, anyone that wants to respond?

Mr. LIVINGOOD. Sure, I can go first, and I will try to be quick so that others can answer. In terms of the positive things that government can do, I think making information sharing easier, there are a number of things there to help. I think that government has a role to play in education, whether that is PSAs or other kinds of education for, you know, end users, for citizens. I think there is also an opportunity to help incent or fund additional R&D. I know that NIST and other groups try to do research and security and other Internet futures. I think there is more than can be done there that is important.

And in terms of things to be careful of or be aware of, I think it is to be aware of mandates and be careful of mandates. I think we don't want to be focused on checklists and compliance. We want to be focused on innovation and the threats of tomorrow, not sort of the threat today.

Mrs. BLACKBURN. Thank you. Anyone else?

Mr. OLSEN. Well, I could just make two comments. Several of the questions and comments today mentioned incentives. I can tell you as an IT professional, we are heavily incented to make sure that we are protecting not only our internal resources but all of our partners that are interconnected with our systems. I think one of the things that is a little scary so far is, we monitor all of our customer service channels, our call centers, stores, Web site, and we are not seeing a lot of requests from our customers concerning their own security of their handsets and devices. So I think education is certainly going to be important. I think there is just not a general awareness in the consumer population how big an issue this is.

Mrs. BLACKBURN. OK.

Mr. MAHON. Maybe a comment more around why it is so difficult to regulate this arena. We have been speaking here rather generically about mobile devices and cybersecurity threats, but it is a much broader problem depending on what category you are looking at and because there are multiple categories of threat actors trying to be—finding a solution in a prescriptive way is very difficult. If you think about who is coming at you and why they are coming at you, you could have a nation-state coming at you for all sorts of reasons. They could be coming at the Federal Government for military reasons, but that same nation-state could be coming after a corporation for intellectual property, everything from under-

standing that that intellectual property is not just a 50,000 corporate environment, it could be in a 50-person law firm doing your M&A activity for you. So you have that broad landscape if you are looking at nation-states.

If you are looking at criminal activity, sure, you have what used to be the script kiddy doing something that was relatively harmless and maybe at best you have hired them today as your network administrator if they grew up, but on the other hand, you have organized crime looking at more broadly the world and how does it make money. If you look at the recent FBI investigation of the DNS-changer malware that infected hundreds of thousands of computers, then you can take a look at your anonymous and others that are more hactivists trying to make a point, and then you come down to your insider threat in your companies that are doing it to you.

So if you think about that landscape and the data that they are after, they are after it for sometimes different reasons. When you try to put a regulatory overlay on that, it is very difficult to put us in a position to respond to those kind of four broad categories, and then at the same time make sure we have our checklist compliance programs going. Thank you.

Mrs. BLACKBURN. Thank you. Yield back.

Mr. WALDEN. The gentlelady is yielding back and now recognize the gentlewoman from the Virgin Islands, Dr. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. Good morning, everyone. Thank you for being here.

I have a couple of questions. Let me begin with Mr. Amoroso. You suggest in your testimony that Congress define the roles of the various executive branch agency in cybersecurity. Where do you see the FCC as an independent agency playing a role?

Mr. AMOROSO. Well, I don't—I mean, I don't think there is an agency right now that is in a good position to come in and solve a problem that we can't solve ourselves. I mean, if it really was the case where you could write out these five things that we should all be doing and for whatever reason—negligence, ignorance, whatever—we are not doing it, then you really do need somebody in government to shake us, you know, into action. The problem is that we don't know what it is that you should be telling us we should be doing. That is why we are pointing to innovation as the key. So it is almost kind of a moot question, whether it should be DHS or FCC or whomever because I am not really sure what they should be telling us. That is the problem. And there are some things, like I said, I am part of the team trying to make recommendations. I am not—you know, I don't want to lead you to believe that we are just kind of punting. It is such a hard problem. But I would just say from an agency perspective, if there was an obvious set of things that should be done right now, I am kind of thinking the groups that are here would be doing it. You know, we are incented to do that. That is the problem. So I hope that addresses the question.

Mrs. CHRISTENSEN. OK. Yes, thank you for that answer.

Mr. Livingood, you mentioned that Comcast is an active participant on the FCC's Communications Security, Reliability and Interoperability Council. So could you just describe for us how you envi-

sion the council's contributing to the improvements in cybersecurity, especially with respect to the types of attacks that the council is addressing—botnets, Internet route hijacking, the main name fraud, et cetera?

Mr. LIVINGOOD. Sure. There are a number of working groups. I am on one. One of the folks that works for me, Mike here, is a chair of one of them, and they focus on things like the security of the routing infrastructure, DNSSEC and a whole range of other things, and I think that, you know, that is a process that works pretty well. People voluntarily get involved and they work together on what they think the current best practices are, and that is a process that repeats regularly every year so that it is not static and it is not sort of—you know, in 2008, we came up with some best practices and that is what we are still focused on. It is something that gets renewed and refreshed all the time and so we can look at every new threat as it comes out, and that is one of many places that we all work together. You know, there are lots of others—the North American Network Operators Group, Message Anti-Abuse Working Group and a whole range of others, other acronyms that I could go on for minutes about. But I think groups like that are good because they are consensus-based, they are voluntary and they are focused on best practices and really current issues.

Mrs. CHRISTENSEN. And while your customers are mainly using your service for in-home computers, they also use the WiFi networks and cellular networks to access Comcast email and other Comcast video products, so how do you continue to ensure the same cybersecurity protections you develop for your core services extend to these uses as well?

Mr. LIVINGOOD. So a number of our security protections are things that a customer can download and install on their device like their home computer, but we have a bunch of things that are on our network like our Constant Guard system, which is a bot intelligence and other security threat system, and that is there for customers that might just be bringing a device into their network, maybe it is a friend that is visiting their house and they are on their WiFi network and they happen to talk, say, a botnet, you know, we will see those kinds of things. And so, you know, we can alert customers to that. So whether they have installed software that we have provided on their device or not, we still have tools in the toolbox to identify that and help them—you know, tell them about it and help to solve it.

Mrs. CHRISTENSEN. Mr. Amoroso, you stress the need to foster informations sharing, and we have talked about that a lot here between the government and private industry as well as among private companies. What protections do you think are necessary to protect civil liberties and consumer privacy, and what do you believe would be the reasonable boundaries to liability protections and antitrust exceptions?

Mr. AMOROSO. Well, the issues you raised are the reason we have those impediments now because, I mean, I am an American, I want civil liberties, I want all those things, so that is the current state, that we have swung the pendulum in the direction of making absolutely certain that we are protecting civil liberties. That is a good thing. So the question is, how do we somehow preserve those lib-

erties and also allow all of us, you know, to know if there is some malware thing. I really think we have to figure that one out. I am not sure I can give you a real good answer on how we do it, but I think it has to be a pretty high priority because the motivation, everybody's shakes and goes yes, if there is not malware, there is not really a civil liberties issue, Comcast should know that blah, blah, blah is a problem and they can code that into their system.

So somehow we just have to maybe get the lawyers out of the room and come up with some kind of a commonsense approach. But that is the reason, all the things you listed. That is why we can't take those signatures today.

Mrs. CHRISTENSEN. Thank you.

Thank you, Mr. Chairman.

Mr. WALDEN. Thank you, Dr. Christensen.

Dr. Amoroso, you should have seen the people shake behind you when you said get the lawyers out of the room.

Let us go to Mr. Bass from New Hampshire.

Mr. BASS. Thank you very much, Mr. Chairman.

I have a couple questions for Mr. Livingood, but before I ask those questions, can I ask a mobile or smartphone question for dummies? Is there a difference in cybersecurity issues between an iPad or a smart device like this and a laptop or desktop computer? Make it quick, because I want to ask some other questions. Can anybody answer that question for me?

Mr. AMOROSO. Well, there is probably a firewall between your PC at work or something on a wired land so we can do more filtering and policy control. With your wireless, you go direct to us, to the ISP, and we have been incented and led, you know, particularly in Washington, push the packets, don't look at them, don't do anything, God forbid you impose any kind of policy or filtering, so we do nothing, so your connection from wireless is directly to the Internet whereas your wired connection probably has some IT group at work.

Mr. BASS. So is this unit here exposed to bots and—is there a cybersecurity issue associated with my iPad?

Mr. AMOROSO. I don't know what you are connected to, but yes.

Mr. BASS. Well, let us say I am connected to Comcast, which is what I am connected to.

Mr. LIVINGOOD. Yes, there sure are those issues and, you know, I think those are a new class of device, and a lot of the hackers and other criminals, they are very focused on return on investment. They are focused where the biggest platforms are and so the more that those devices get out there, the bigger target that makes and so they will see, OK, I can spend a couple of days developing this and I have got a few million devices. So you will start to see more and more of those things, and depending upon the tablet that you have, some are more vulnerable at the moment than others, but, you know, that is something that a lot of Americans are buying and so that will be the next threat. It will be those type of devices.

Mr. BASS. Who is responsible? Is Apple responsible for this or are you?

Mr. LIVINGOOD. Well, I think it is a variety, so I think with that device, Apple plays a role. With the Android devices, Google plays a role. And then all the software vendors that make the apps that

go on that play a role. But there is also a component of customer education, and I am sure over time, you know, just in the same way that we have software that runs on PCs to provide security, you know, that is going to start to develop and evolve for tablets and provide that extra level of security as well. We are at the early stages of that adoption curve.

Mr. BASS. And the same is true for BlackBerry, right?

Mr. TOTZKE. Well, I mean, all of the tablets are going to have different risks and different threats, and we look at it in terms of how we protect our platform. But the theme that I keep hearing over and over, and I think it is one that this committee has really highlighted, is the need for education, right, and when you talk about computer security, one of the inevitable comparisons is to driving a car, right? We don't let people drive a car without a license but we let them get on the computer, connect to the Internet and download software without really understanding what those risks are, and that piece of education—I am not suggesting we license people to use a computer but we do need a level of sophistication and education in how we inform people of risks that they have when they connect a device.

Mr. BASS. Fair enough. I just want to ask a couple questions about the Constant Guard Protection Suite. I note in your testimony, Mr. Livingood, on page 6, it says "At Comcast, we understand that securing cyberspace is a complex task" and so forth. "Education, prevention, detection, remediation and recovery are the core objectives of our anti-malware efforts." Does Comcast require its customers to download the Constant Guard Protection Suite, and if not, how is the customer going to know that it exists and how are you going to notify them that they have a problem?

Mr. LIVINGOOD. So it is not required that a customer download that to use our service. You know, they just have to have normal Internet connectivity to do that. But we do a lot to make customers aware of that and to incent them to download it both before they have an issue and after. So before they have an issue, you know, when they are installed, they are given a lot of information about the things that are available for them and they are given links to that and so on. When they get a welcome email from us when they sign up for service, we are reiterating that for them. And we do a lot of things on our Web site and other places to promote the fact that these are available. Certainly after they have an issue and we notice it, we drive them to a remediation portal, and that is one of the first things that we recommend that they download is that suite and we take a number of other steps. So we do a lot of education upfront. We do a lot when they come on. We call it onboarding when they come on as a customer. And we do things while they are a customer to keep reiterating that and then afterwards.

Mr. BASS. Real quick. It is limited to Windows operating system, correct? How long has it been around?

Mr. LIVINGOOD. That protection suite is pretty recent. I think that is a little bit more than a year. That is a supplement to a larger anti-virus and security suite that we have had for many, many years that is——

Mr. BASS. And real quick, because I have run out of time. What business incentives, if any, did you get or did you have in developing and offering this service?

Mr. LIVINGOOD. Well, we view it in two ways. Number one, there is a competitive incentive if we can be seen as having more security features or more secure than the next guy, someone chooses us as their ISP rather than someone else, but the other thing is that customers when they come on board as a customer used to tell us that the two reasons were price and speed, and today, it is price, speed and security. So customers are very aware increasingly so, not aware as they need to be but very aware these days about security. They ask about those things when they call us up to order service. And so we view it as a competitive feature that we need to add, and that is why all of the things that we are doing as part of Constant Guard, DNSSEC and other things, are important to us.

Mr. BASS. Thank you, Mr. Chairman.

Mr. WALDEN. Thank you.

Now we go to Chairman Dingell for 5 minutes.

Mr. DINGELL. Mr. Chairman, thank you.

Gentlemen, we have much to do in little time, so I am going to try to ask questions that you will answer yes or no to starting now with Mr. Livingood. Gentlemen, you all seem to be in agreement that imposing new Federal cybersecurity regulations on industry would stifle innovation and harm industry's ability to protect consumers from cyber threats. Is that correct, yes or no, starting with you, Mr. Livingood.

Mr. LIVINGOOD. Yes, I am concerned about that.

Mr. DINGELL. Mr. Amoroso?

Mr. AMOROSO. Yes.

Mr. DINGELL. Sir?

Mr. MAHON. Yes.

Mr. DINGELL. Sir?

Mr. OLSEN. Yes.

Mr. TOTZKE. Yes.

Mr. DINGELL. Now, gentlemen, let us assume for a moment that the Congress will pursue the no-regulation path in this matter and instead facilitates greater information sharing about cyber threats between industry and the government. Would that be your collective preference? Yes or no.

Mr. LIVINGOOD. Yes.

Mr. DINGELL. Sir?

Mr. AMOROSO. Yes.

Mr. MAHON. Yes.

Mr. OLSEN. Yes.

Mr. TOTZKE. I would agree.

Mr. DINGELL. Gentlemen, thank you. In that case, would the Congress need to consider granting exemptions to the antitrust laws and the Federal Trade Commission Act in order to allow the companies to share cybersecurity information amongst themselves? Yes or no.

Mr. LIVINGOOD. Yes.

Mr. AMOROSO. Yes, I think that is correct.

Mr. MAHON. Yes.

Mr. OLSEN. Yes.

Mr. TOTZKE. I unfortunately can't comment on that.

Mr. DINGELL. Very good. Now, gentlemen, similarly, do you believe that a safe harbor provision should be created in statute to permit companies to share serious cyber threat information with government agencies without fear of class action or other lawsuits being brought against them? Yes or no.

Mr. LIVINGOOD. Yes.

Mr. AMOROSO. Yes.

Mr. DINGELL. The reporter doesn't have a nod button, sir, so you have to say yes or no.

Mr. MAHON. It is a yes.

Mr. DINGELL. Thank you.

Sir?

Mr. OLSEN. Yes.

Mr. TOTZKE. I am afraid I can't comment on that. I don't know.

Mr. DINGELL. Now, gentlemen, my last several questions have been premised on a no-regulation scenario wherein the Congress adopts legislation to promote information sharing between industry and government. Would you please submit for the record what enforcement tools you believe the Federal Government would have in this scenario to ensure that industry is adequately guarding and being guarded against cyber threats? I am asking to make a submission there for the record because of the shortness of time.

Now, gentlemen, let us assume that the government would have some role in promoting cybersecurity in the private sector. If the Federal Government were to require the promulgation of cybersecurity standards, should such standards preempt State laws? Starting with you, Mr. Livingood, yes or no?

Mr. LIVINGOOD. Yes. It is easier to have one standard.

Mr. AMOROSO. Yes, I don't know. I am not sure. I haven't really thought that one through.

Mr. DINGELL. And you, sir?

Mr. MAHON. Yes.

Mr. DINGELL. Sir?

Mr. OLSEN. I will have to agree with Dr. Amoroso. I haven't really considered that.

Mr. TOTZKE. Yes, and I can't comment on that either.

Mr. DINGELL. Now, gentlemen, I have read with some interest in Mr. Olsen's testimony that, and I quote, "the ongoing evaluation or MetroPCS's security program is based on periodic internal and third-party assessments and auditing." Would your respective companies object if such audits were government mandated? Yes or no.

Mr. LIVINGOOD. No, we already provide all those things already. We already do that.

Mr. AMOROSO. I think we would object, yes.

Mr. MAHON. We would object.

Mr. DINGELL. You would object?

Mr. TOTZKE. Yes, we would.

Mr. DINGELL. All right. And then let me come back and ask you to explain that, if you please?

Mr. TOTZKE. Yes, we would probably object but we do this anyway. We always do that.

Mr. DINGELL. Now, those who have indicated no, would you please explain briefly?

Mr. AMOROSO. I can explain. When you write a law, we do paperwork, so I take people away from doing their day-to-day work to sit and do work. We have an ops lab, and one of our favorite things to show people in the ops lab is along one of the walls, we have got about a mile's worth of ring binders and they always say there is the government paperwork followed by a lot of sort of chuckling laughter, but it is true. You know, we do have a great of paperwork that we fill out, you know, when we are dealing with different Federal groups or Sarbanes-Oxley or whatever. There is a lot of paperwork, so I am just suggesting that if we are already doing it and government comes in and says I need you to fill out this compliance checklist, you are taking people away from the work to do paperwork. That is why we would object.

Mr. LIVINGOOD. Very quickly, if I can just make a note very quickly. I think this is dangerous sending an engineer sometimes, but I am told that we might have objections. We would object and have the same concerns.

Mr. DINGELL. Gentlemen, thank you.

Mr. Chairman, thank you for your courtesy.

Mr. WALDEN. Mr. Chairman, thank you for your questions. I think you got to the heart of the matter quickly.

We now turn to the chairman of the House Intelligence Committee and a very important member of our subcommittee, Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman. Thanks for having the hearing. Thanks to the witnesses as well.

I think one of the big problems that we run into in this is that we haven't really sounded the alarm bell. I think in all of the circles of people who look at this every day, all the security shops, the IT security shops across America, they know what the problem is. Average users don't see it, and that is why there is no hew and cry, I think, yet about how we get this fixed. But I appreciate all your comments today.

You talked, each of you, about the importance of information sharing and keeping it as clean and simple as you can. Talk about how that would work. So if we bring the folks together, we are sharing the government secret sauce with you all and you are sharing back malicious ware that maybe the government is not aware of, talk about how fast this is. There is a lot of talk about civil liberties, and I think people have this visual that people are reading emails, some guy named Bob in Cleveland is reading everybody's email to find this malicious software. It is not how it works. As a matter of fact, if that happens, it is a miserable failure. Can you talk just a little bit about how you envision that that would with the sharing arrangement, real time, no regulatory, all voluntary? Can you talk about that quickly?

Mr. AMOROSO. Yes, I would be happy to. First of all, I want to compliment you on your legislation. I think that there is some real nice elements in the work you have done. First of all, real time, absolutely. Independent auditable, I think is important so that somebody can come in and look a the way this is done, but it also has to be controlled like blasting it out, you know, over the Internet would be a really bad idea but I think you need the balance, right, this real time but also the ability to come back and look at the

process, make sure it is transparent without, like I said, exposing it to our adversaries. That is the right way to do it.

Mr. MAHON. There is also different levels of sharing by industry. I think you have to look at how you do your risk assessments on each category that I previously described but there is also right now a very good example out there of what is working well, and that is the defense industrial base pilot that is going on, and that particularly is supporting defense contractors and DOD, but you can expand that to the financial services industry and other industries.

Mr. ROGERS. And just for clarification, when we talk about real time, I have seen numbers as high as 100 million a second, the packets of information flying around. So if this is going to work, the malicious source code has to be compared at an incredibly fast rate. Can you talk about that from an engineering perspective? Anyone?

Mr. LIVINGOOD. So I think one of the challenges is trying to do any kind of pattern matching. A lot of the malware that we see and have seen for a number of years is sort of what is called polymorphic where it changes. Every individual, you know, instance of it is different from the next so a lot of stuff changes. It is not like it is with anti-spam where you can match on a few key words or a file attachment and know, you know, that is it, that they target and flag it that way. So you need to come up with ways, and a number of us have systems like this and there are others that are in development that can do this on a wider basis, but that is the very challenge that you are getting at, which is doing that in real time. It is incredibly difficult and you are at the edge of computer science at that point.

Mr. ROGERS. Which is why I think many of you have told us before the legislation was written, be careful about the regulatory scheme. If we slow you down, if we give you another row of books down your mile-long hallway there, it doesn't work. I mean, we already have outdated what you are trying to accomplish in the room, and this is a value added not only for you but for the government, is it not? The government also gets benefit from the protection of all of your great work in the private sector, correct?

Mr. LIVINGOOD. That is correct, and there are two things that I think that raises that are interesting. One is, by the time that a very prescriptive law would be written, by the time that ink was dry, the threats would have moved on and so you have got to be able to be flexible. The other is that we all need to have, you know, with our software developers and security specialists, you know, they need to be hard at work in a room, not with half a room full of lawyers with them slowing them down and asking questions about, you know, why are you doing this and that. They need to be at work every day trying to solve this problem.

Mr. ROGERS. And I have to say for the record, this may be my favorite panel of all time since I have been in Congress. Never so often have a group of engineers belittled lawyers at the table. You have warmed my heart today. We have faith that we are moving forward.

I wish we had time to talk about all the issues. I am very curious about how you would fix the programming issue, a huge problem

for us as we move forward. We didn't talk about exfiltration, which is very difficult for any of you to catch, which I would argue right now is the single greatest threat to our economy moving forward, aside of the things that we know today.

Mr. WALDEN. Would the gentleman yield?

Mr. ROGERS. Yes.

Mr. WALDEN. Could you outline exfiltration?

Mr. ROGERS. Sure. It is—we know that nation-states today are engaged in getting on to your network lurking. They will be there for a very long time. You don't know it. Your system administrators don't know it. These folks can't catch it. Sometimes the government—a lot of times the government can't catch it either. And then they will latch on to that intellectual property that is on everybody's computer today, all those designs, everything that is of value to that company, and at the right time at the right speed, they latch on to it and run like heck through your network and take it back. And we know a country like China, who is investing in this as a national strategy to exfiltrate intellectual property and then directly use that intellectual property to compete against United States businesses, and unfortunately, it is happening at a breathtaking pace, breathtaking pace, and what is concerning is, these folks are looking for malicious software that is disruptive or theft-oriented. This is very sophisticated, as sophisticated as any you will see, and incredibly hard to detect, and they really don't want to break anything. They want to get in and steal it without you knowing it, and that is what is so troubling about it.

Hundreds and hundreds of thousands of jobs are lost every year for the theft of that intellectual property that is being reprogrammed commercially against U.S. companies. This is as big a problem as I have ever seen and it is one of the many things that keeps me up at night, Mr. Chairman, so thanks for letting me explain it, and it is something we didn't really get into today because that is really not the focus of what they can even watch. So that is why this information sharing I think is so important. It would help American businesses by the Federal Government having information and being able to identify that code, share it with the right partners. It is amazing what we would be able to stop.

Mr. WALDEN. With the indulgence of the committee members, perhaps given the importance of that topic you could each if you have anything you want to add on that area, and then we will go to Mr. Stearns and Mr. Gingrey. Does anybody want to comment on that?

Mr. AMOROSO. I will. It is called advanced persistent threat, and he has got it exactly right. It is somebody targeting any of you, like we know the folks that you run around with, we can craft a fake email that looks pretty realistic, point you to one of these Web sites that establishes a tunnel. It drops a remote access tool on your PC. You know how you log in when you do remote access from work or from home, wherever you are doing it? This is the hacker now doing remote access to you. You are now the server, and once they are on, they can troll around your PC, your network and so on, and the intellectual property theft has become significant. It is probably the number one thing I bet all of us, you know, when we go back, we talk about bot nets here and we talk about DNS, but that is

not what we deal with when we go back to the office. We are dealing with APT, which is kind of our point, right? We are ahead of the discussions here, things that we have been dealing with in the past and the things we deal with now are probably things we will be here testifying about 5 years from now, so that is an issue.

Mr. TOTZKE. And just to echo Dr. Amoroso, the advanced persistent threat, I mean, these are remarkably sophisticated adversaries. They are slow. They are patient. They will lurk on your network for years. And, you know, I came from our Canadian headquarters. We had a large company go out of business, Nortel, and part of the attribution of that is loss of their intellectual property to a foreign State-level adversary, you know, siphoning secrets right off their network.

So when you look at that, this is a serious concern. As Ed mentioned, 5 years from now, you will probably be looking at that. That is how advanced they are. It is great that you are looking at it now, Congressman, because the threat is real, it is persistent today, and as you stated, it is a threat to jobs and it is an economic threat to the United States and elsewhere.

Mr. WALDEN. Thank you.

Mr. ROGERS. Thank you, Mr. Chairman, and just for the record, I want to thank Mr. Mahon for his 30 years of FBI service as well. Thank you for all the time you have put on the target, sir. Thank you.

Mr. MAHON. Thank you.

Mr. WALDEN. You would think Rogers was a former FBI agent himself.

Let us go to Mr. Stearns now.

Mr. STEARNS. Thank you, Mr. Chairman.

Let me take my questions a little bit along the lines that my colleague from Michigan talked about when he talked about advanced persistent threat. Dr. Amoroso, when you did your opening statement, you were speaking quite eloquently in talking about malicious software, malware, you talked about, and you painted this picture that the malware itself you were impressed how well it was developed, put together, and you sort of alluded to the fact that it was almost not unpenetratable but it was to the point you were respectful of it and were not sure we were keeping up. Is that my interpretation of what you said?

Mr. AMOROSO. That is exactly right. We are definitely not keeping up. We are trying. But think of the dizzying pace of innovation that you see out in Silicon Valley, right? I mean, new things every day. The hacking and the malicious adversary community, they are moving at the same pace so the job we have is, we have got to keep up, and you would say hey, guys, you better be ahead of them like not even enough to just kind of keep up, you better be ahead. So we are always going to be sort of biased.

Mr. STEARNS. So you are saying you are always catching up?

Mr. AMOROSO. Let us go faster. We have to innovate. We have to go faster.

Mr. STEARNS. Is that true, you think you are always catching up then? That is what you implied to me by saying the respectability you had for this malware.

Mr. AMOROSO. Yes.

Mr. STEARNS. Is this true for adware, spyware, grayware, all these others? Is it also applicable to that too?

Mr. AMOROSO. Yes. APTs are the best, right? I mean, APT, this exfiltration point that the Congressman spoke about, that is the elite kind of attack vector in 2012.

Mr. STEARNS. OK.

Mr. AMOROSO. Spyware, maybe not so much.

Mr. STEARNS. Now, with the malware, who are these people that are doing this specifically? Can you name them?

Mr. AMOROSO. I can't. I am not law enforcement. You might——

Mr. STEARNS. Is there anybody on the panel—when Dr. Amoroso talked about this malware so respectfully and how eloquently it is put together, can anybody tell who we are talking about?

Mr. MAHON. I think if you take a look at the most recent investigation conducted by the FBI on the DNS malware, you will see that was a group of individuals operating out of Estonia that basically sent malware to individuals in various forms in emails, and you clicked on it and it infected your computer in a way that it directed you when you went out to do a DNS-type search, you were looking for, I don't know, Amazon.com or some other company, you really went to their servers and their own servers were actually embedded in various locations in the United States.

So these are organized crimes. They have figured out how to capitalize on the money you can make with the malware.

Mr. STEARNS. Are these people, for example in Estonia, are they part of a mafia, underground, an organization that is larger that just in Estonia, without you revealing any——

Mr. MAHON. These are no longer just individual hackers. Individual hackers are out there but now they have actually formed themselves into types of federations to work together.

Mr. STEARNS. Across the world?

Mr. MAHON. You can do it across the world. There are a certain hacking groups you can join and be a member from different countries.

Mr. STEARNS. So it is like a fraternity? You say I am a member of the Estonia——

Mr. MAHON. Estonia just seems to be a hotbed right now, I think because of how the economy is run over there.

Mr. STEARNS. Anyone else?

Mr. LIVINGOOD. If I could add to that, I think it is actually pretty interesting. This is a very large and very well organized underground economy. They are specialized. They have some people that write tools, other people that rent access to bot networks so you can rent botnets by the hour. You can tell them where you want people—where you want the bots to be, what kind of computers, you know, payment network mechanisms between these parties. So it is very sophisticated and, you know, if you think about from a criminal standpoint, it is a lot easier to get a return on investment on this type of thing than it is to go out and do physically oriented sort of crimes, and the scale is so much larger. These are folks that operate across borders internationally and there is just an enormous amount of, you know, economic incentive for them to do it, and it unlike APT, at least in some respects, this is primarily an economic crime. APT is focused certainly on economics but more on

intellectual property or embarrassing companies. This is all about the money.

Mr. STEARNS. Well, I guess, Mr. Mahon, is there a possibility that we have terrorists involved with this that are part of Estonia? The terrorists could go to this group or this federation across and are using them? Is that——

Mr. MAHON. Absolutely. Terrorists use these types of schemes for funding. Number one, they need funding for their operations. And number two, they use it just as a communications system. They know they are being looked at. So the ways they need to communicate are surreptitiously in a manner that they can't be intercepted, so they use these types of technologies to communicate with one another, but they have to fund their operations.

Mr. STEARNS. I guess the basic question is, and this is probably the premise of understanding what this hearing is all about, what could we as legislators on this subcommittee or the full committee or Members of Congress, what can we do to make it easier for you to operate and at the same time give you the wherewithal to compete and what should we not do? What should we do and what should we not do? And just as a closing statement, Mr. Livingood, if we could just go down the panel and each give what we should do and what we should not do, that would be helpful.

Mr. LIVINGOOD. Sure, of course. I think what you should do is help make information sharing easier, remove those impediments. I think also there is a role for government to play in education, whether that is PSAs or other things, to raise awareness about security issues, and I think that there are R&D types of things through agencies that you can help fund to focus on this.

I think what you should not do is focus on mandates and compliance. That enables us to focus instead on innovation.

Mr. AMOROSO. That sounded good. I would exactly repeat those comments. I will add one additional, and that is that you do have some influence around the Federal procurement process, so a lot of times we see procurements come out and we scratch our heads and say don't you think there ought to be, you know, like through GSA there is this MTIPS program, a lot of us are MTIPS vendors. There ought to be more business. There isn't. So I would recommend that that procurement process ought to be the most secure process in the entire world.

Mr. MAHON. You know, I would echo what both of them said and just add the importance of information sharing. We have limited resources. We conduct risk assessments when we are trying to decide on impacts and probability of events based upon the information we have at the time. If a government agency or another carrier has additional information and we don't factor that into our analysis, we are really misaligning our resources and how we develop our countermeasures.

Mr. OLSEN. I think there is a lot of commonality among the panel here on what we would like to see. I think just add a little bit to the information-sharing area. I think the Federal Government has access to information through various agencies that are watching the country's cyber borders and we have seen in our company the vast majority of reconnaissance scams and attempts to gain access are coming from China and Eastern Europe, and I think the Fed-

eral Government would be in a good position to monitor and provide more information on that.

Mr. TOTZKE. Going last, I get to say I agree with everybody else on the panel here, especially I want to hammer that information sharing from government to industry. The purview that intelligence agencies have and that you have in terms of what you see is much different than what we see. So my team works with Dr. Amoroso's team on areas of commonality between RIM and AT&T where we think we have issues that need to be addressed that impact the security of our customers but we don't necessary get that feedback from the government about what do you see that we need to be aware of, and if there is anything I could ask for, it is a more transparent, more real-time information-sharing mechanism to let industry know what government knows so we can act to protect out networks and by extension protect your information.

Mr. WALDEN. Thank you.

Mr. Gingrey, thanks for your patience as we have gone through the hearing. You are the last——

Mr. GINGREY. Mr. Chairman, you took the words right out of my mouth. I think you are exacting the last measure of patience out of the last member to ask a question, but I moved down here early in the hearing, as all of you know, because I couldn't hear very well, even though the chairman said speak right into your microphones, but I am glad I did move down close because I knew it was going to be interesting and I know that all five of you are experts who were going to have a lot of useful information to present to us, and quite honestly, after 2 hours of this, I am trying to figure out a way to beat these guys, and the only thing I can think of is an opportunity to invest in these hacking operations. I don't guess that would be legal, but if it were, I think that would probably be one of the best ways for us to win. Thank you all very much.

Let me ask a couple of specific questions, and maybe this cuts a little bit to the chase of one of the main reasons why the chairman is holding this hearing, and each one of you, please, starting with Mr. Livingood, answer this for me. Do you believe the FCC has enough cybersecurity expertise to allay the concerns that some industry stakeholders have with the Commission? If they do choose to impose cybersecurity regulations on you guys, on the network providers, do you have enough confidence in their expertise to do that, Mr. Livingood?

Mr. LIVINGOOD. So I don't know the answer to that. You know, we work with a lot of folks at the FCC and enjoy doing that. They have a lot of expertise. Whether they have enough here, I think that is a tough question. I don't know the answer.

Mr. AMOROSO. I have said earlier, I don't think there is any agency that has the right expertise to do that. If we knew what the answer was, we would be doing it, so I don't think it is a knock on any one particular agency. I just don't think there is any agency that has that capability right now.

Mr. GINGREY. Mr. Mahon?

Mr. MAHON. And I would agree with Ed. The answer is no. But I don't think anyone does, and I think that is the importance of collaborative relationships. You do need to bring people in from all sorts, the Federal arena as well as the private industry area to

work together due to the evolving nature of the threats in this arena.

Mr. GINGREY. Mr. Olsen?

Mr. OLSEN. Yes, it is an important question, but I would have to agree with Mr. Livingood. I don't know whether they do or not.

Mr. GINGREY. Mr. Totzke?

Mr. TOTZKE. Yes, I don't actually know either. I think what you are hearing here, and it is common amongst the panel, is the defender job, the job that we are trying to do to protect your information, is exceptionally hard and it is actually much more difficult than being on the other side.

Mr. GINGREY. Yes, speaking of hedge funds.

Let me go back to Mr. Olsen. In your formal testimony that you gave, you talked about the clearinghouse. I would like to know a little bit more about that specifically, and do you think that would be helpful? And maybe you could elaborate a little bit more on that.

Mr. OLSEN. I think there is really two aspects to that. One is where the Federal Government is sharing with private sector, with industry, what they are seeing as far as threats, and I mentioned a little while ago about the threats from outside the United States, so I think that is a critical component. The other is where companies should share, private companies could share information on threats that they are seeing and that clearinghouse would have to be sponsored by somebody, and I think the Federal Government is really the right place to do that.

Mr. GINGREY. And I think you addressed also in your testimony the hold-harmless provision that would be necessary to share that information so that you wouldn't be subject to lawsuits and that sort of thing.

Mr. OLSEN. Yes, sir.

Mr. GINGREY. I have got a little time left. I have one more question then. The Internet is currently transitioning from this Internet provider v4 to v6 addressing. Does that process create any new cybersecurity issues, and will transitioning alone solve any cybersecurity issues that currently exist? Does the process of transitioning present opportunities to resolve existing cybersecurity issues? We will start with Mr. Livingood and just go down the line.

Mr. LIVINGOOD. Sure. I think, you know, we have been a leader in IPv6. You know, I think that all of those issues that exist in the current Internet and IPv4 simply carry over to IPv6. It is just a new form of addressing. You know, that being said, because it is a new form of addressing a new technology, you are introducing new things into the ecosystem. To Dr. Amoroso's point earlier, it is a complex ecosystem. When you change something, it can have unintended consequences. And so it is something that you have to keep an eye on and make sure that you are not introducing any new vulnerabilities. But I think if there were any, it is simply because, you know, some security that worked great in IPv4 might not have all the same features.

Mr. GINGREY. Dr. Amoroso?

Mr. AMOROSO. Every device on the planet running v6 in theory would be addressable, would be routable, and that is a pretty dangerous situation, so for all of us, we have to figure out how to archi-

tect security protections around that. So I do have some concerns about the v6 transition.

Mr. GINGREY. Mr. Mahon?

Mr. MAHON. Yes, the architect and engineering teams are still working through this, but as they have said, you have legacy systems being married up with new evolving technology, and whenever you do that, you are going to have things evolve as you begin to deploy it.

Mr. GINGREY. Mr. Olsen?

Mr. OLSEN. I think from a protection standpoint, I think it is a step ahead, but the bad guys are out there working just as hard as we are to find another way around that, so as soon as we make an advancement in technology, they are right out there keeping pace with us.

Mr. GINGREY. And finally, Mr. Totzke?

Mr. TOTZKE. And this just, as Ed said, expands the attack surface and by doing so increases the risk, so we have new and unknown risks that we are going to have to figure out how to mitigate.

Mr. GINGREY. Mr. Chairman, thank you for your generosity of those 45 extra seconds, and I will yield back.

Mr. WALDEN. Actually, you got close to 49. Thank you, Mr. Gingrey, for staying and participating.

I want to thank all of our witnesses and all the folks behind them who I am sure played some role, but we really appreciate your insights. It is very helpful in our effort. Obviously, we are trying to do the right thing and you are out there fighting the battle every day, and we don't want to get in your way. And so we may be back to you with our working group digging a little deeper on some of these issues and getting as specific as possible. We hope to look out too at some of the other types of networks and small providers. I mean, you obviously represent major providers or a representation of them. We are also wondering about the weakest link, which might be small ISPs and how do they deal with this and do they have the same sorts of capabilities to fight back.

Anyway, I deeply appreciate your willingness to be here today and share your knowledge with us. We are better for it.

So with that, the Subcommittee on Communications and Technology stands adjourned.

[Whereupon, at 12:13 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record 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

June 11, 2012

Mr. Jason Livingood
Vice President, Internet Systems Engineering
Comcast Corporation
One Comcast Centre
Philadelphia, PA 19103

Dear Mr. Livingood,

Thank you for appearing before the Subcommittee on Communications and Technology on March 7, 2012, to testify at the hearing entitled "Cybersecurity: The Pivotal Role of Communications Networks."

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

RESPONSE TO QUESTIONS FOR RECORD FROM HON. ANNA ESHOO

1. I believe that the integrity of the supply chain is essential to the security of our nation's communications networks. Do you share these concerns? If so, what role should the Federal government, including the FCC play to ensure supply chain security?

A. We agree that supply chain integrity is an important issue. Comcast has very robust procurement protocols and safeguards in place aimed at ensuring the integrity of our supply chain, and the equipment and software we acquire. That is a business necessity for us. While it may be advisable for the Federal government to have its own set of procurement protocols that ensure supply chain integrity in place in connection with acquisition of equipment for Federal agencies, imposing such rules on the private sector is neither necessary nor productive. The marketplace consequences – in terms of loss of trust and damage to reputation – offer network providers ample incentive to ensure the integrity of their supply chain.

2. How do we ensure private sector commitment to a voluntary ISP code of conduct, like the one being proposed by the FCC's Communications, Security, Reliability and Interoperability Council (CSRIC)?

A. Comcast has been deeply involved in CSRIC cybersecurity initiatives because we think it makes business sense to do so. Our customers want assurance that the network they are using is safe and secure. As a result, we have strong incentives to invest capital and resources into cybersecurity safeguards and to take the actions necessary to secure our substantial investments in our networks against cyberthreats. The same is true for other network providers.

The CSRIC is a valuable forum because it draws broad industry participation that in turn generates innovative and useful recommendations. CSRIC's voluntary best practices approach enables companies to adapt those recommendations to their particular network architecture and business model. The flexibility inherent in this voluntary framework is critical, given the constantly evolving business and technology environment in which ISPs compete and the rapidly changing cyber threat landscape. Making CSRIC's recommendations mandatory is unnecessary and could have the unintentional effect of deterring industry participation in this process in the future, out of a concern that they could not implement a particular recommendation.

3. How do service providers avoid using the lowest cost provider of equipment, even if there are risks associated with such a supplier? Is it reasonable to expect them to properly evaluate the supply chain risks associated with an equipment provider?

A. The initial equipment cost is only one, often relatively modest, element to be considered in connection with the decision to procure equipment; initial cost and total cost of ownership over the usable lifetime of equipment are quite different. The quality and reliability of the product and the track record of the vendor are factors that are just as important as cost, if not more so. In addition, the cost and complexity of operating the equipment, the frequency and quality of future upgrades, the ease of integrating new applications, and the ease of monitoring and remote administration are also factors, among countless others. Comcast and other network providers are in the business of providing their customers with a safe, secure and reliable

connection to the Internet and other services, and therefore have strong business incentives to avoid equipment vendors that do not have an established reputation for trustworthiness, reliability, integrity, quality, and other key decision-making factors.

RESPONSE TO QUESTIONS FOR RECORD FROM HON. HENRY WAXMAN

1. Many have expressed a preference for competitive marketplace forces to discipline companies to implement adequate cyber security measures. Concerns have also been expressed about overly prescriptive approaches to regulation. Given the potentially severe consequences to the country of a significant cyber breach, are there any generally applicable mandates that you believe would be constructive? For example, what if some other company that is part of the Internet ecosystem fails to be as diligent as yours and, as a consequence, causes harm to your network, or even harm to a critical infrastructure sector? Should there be some way of holding all stakeholders accountable for employing best practices?

A. The most important thing that Congress can do to enhance cybersecurity readiness and deterrence is to remove uncertainty and legal impediments to the sharing of cyberthreat information among network providers and between the private sector and the government, subject, of course, to appropriate privacy protection. With respect to the implementation of cybersecurity measures, the most effective policy is one that preserves our flexibility to devise the best possible security solutions that are optimally adapted to our particular network architecture and customer environment. Even the most comprehensive and forward-thinking regulation will be likely to restrict or otherwise minimize the overall effectiveness of research and development in the area of cybercrime – energy spent on developing creative and effective solutions will be shifted to focus on regulatory compliance.

Prescriptive rules and enforceable mandates are unnecessary to ensure that network operators implement cybersecurity measures. Network operators have powerful marketplace incentives to take strong and effective measures to ensure network security and safety. Our customers want assurance that the networks they are using are safe and secure, and so we have strong reasons to invest capital and resources into cybersecurity safeguards. The same is true for other network providers. Network operators also have powerful incentives to take the actions necessary to secure their substantial investments in our networks against cyberthreats. The marketplace consequences associated with ignoring or shortchanging cybersecurity issues would be severe.

With respect to the specific example you raise, there are many formal and informal groups that enable network operators to work together for the greater good and to maintain stable connectivity between networks. This includes the FCC's CSRIC, the Broadband Internet Technical Advisory Group (BITAG), the North American Network Operators Group (NANOG), the Messaging-Mobile-Malware Anti-Abuse Working Group (M3AAWG), the Internet Engineering Task Force (IETF), and the Anti-Phishing Working Group (APWG), among other channels. We agree that network operators alone cannot protect and address Internet cyber attacks. The Internet is an ecosystem composed of Internet service providers, edge providers, content developers, and others. The development of a cohesive, effective policy must include

participation and feedback from all of these stakeholders, not just Internet service providers. We are working with industry groups to ensure broad participation by all ecosystem participants.

2. Specifically, concerning mobile devices, especially smart phones and tablets, what are the cybersecurity implications of the wide open apps market, and what is the risk of botnets spreading to mobile devices?

A. The benefits of an open apps marketplace are significant, and this creates much opportunity for innovation and the creation of valuable new applications for consumers. Consumers have long been able to install the applications of their choice on personal computers, and the rise of smartphones and tablets brings that capability these devices. It is safe to assume that the threats that come with this model in personal computers will be similar as new devices become as open and widely adopted, and this is something that we and many other network operators and other players are working on.

However, the strong growth and proliferation of new mobile, smartphone, tablet, and other personal devices that have Internet access highlight the need for a consumer-focused approach to cybersecurity to work in tandem with network tools and protocols. Botnets are typically surreptitiously installed on common consumer devices, so almost any device with a connection to the Internet or a local access network (LAN) can become a vehicle for infection. This is precisely why Comcast has been focusing on conveying to our subscribers the importance of security tools such as our Constant Guard security suite. As public awareness of these issues grows, so, too, does consumer demand for comprehensive security offerings that provide peace of mind as well as a more secure Internet experience.

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

Response of Edward Amoroso, Ph.D.
Senior Vice President & Chief Security Officer, AT&T
to
June 11, 2012 Additional Questions for the Record of the Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses"

The Honorable Anna Eshoo

1. **I believe that the integrity of the supply chain is essential to the security of our nation's communications networks. Do you share these concerns? If so, what role should the Federal government, including the FCC play to ensure supply chain security?**

Answer: AT&T, a global company operating in many jurisdictions and exchanging traffic with entities in virtually every country around the world, relies on a global supply chain. As such, we share these concerns. Given the global nature of the supply chain, and in particular the fact that virtually all communications hardware and much software is developed and/or manufactured off-shore, we believe that our shared concerns over supply chain integrity are best addressed as part of a holistic cyber security strategy that manages the full spectrum of risks to communications network infrastructure.

As part of its strategy to operate the most secure and resilient network infrastructure, AT&T has implemented a trusted supplier program for everything it purchases. At its essence, this encompasses developing long-term, trusted relationships with suppliers in which we continuously evaluate all aspects of the supplier's operations to identify any risks to the AT&T infrastructure inherent in the relationship. As those risks are continuously identified, AT&T implements appropriate risk management and monitoring practices, including operational processes as well as redundancy and diversity in how the supplier's products are implemented in our infrastructure. All components of our infrastructure are put through extensive testing in order to evaluate their performance in normal and stressed conditions, and to identify any security or performance issues. This happens before they are put in service, and they are subject to continuous monitoring afterward.

We believe that the best way that any government agency, including the FCC, can assist the private sector with respect to supply chain integrity is to provide any specific information that it may possess concerning potential supply chain security threats in order to assist companies in their performance of meaningful supply chain risk assessments and management strategies.

2. **How do we ensure private sector commitment to a voluntary ISP code of conduct, like the one being proposed by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC)?**

Answer: Private sector communications providers already have strong incentives, including substantial economic and reputational incentives, to implement effective cybersecurity practices.

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

Response of Edward Amoroso, Ph.D.
Senior Vice President & Chief Security Officer, AT&T
to
June 11, 2012 Additional Questions for the Record of the Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses"

Further, AT&T and other private sector communications providers have a long history of working with the government and other stakeholders to keep the Internet secure through substantial investment and innovation. Indeed, innovation is critical here. Compelling adoption of a specific code may have the unintended consequence of limiting the flexibility of industry to react to constantly emerging evolving threats. Therefore, the best way for the government to encourage private sector commitment and accountability to voluntary codes of conduct is to keep those activities truly voluntary and by doing so encourage collaborative, creative interaction of cyber security professionals throughout the communications ecosystem

3. **How do service providers avoid using the lowest cost provider of equipment, even if there are risks associated with such a supplier? Is it reasonable to expect them to properly evaluate the supply chain risks associated with an equipment provider?**

Answer: As mentioned above, supply chain issues are best managed as part of a comprehensive and continuous cybersecurity risk assessment strategy. For AT&T that means a process that considers all aspects of product acquisition, including total cost of ownership through the expected life-cycle of the product, overall performance and product reliability, results of comparative testing, and long-term experience we have with the vendor, including reputation, financial transparency, and the integrity of their supply chain. In our experience, a product provider presenting unacceptable risks in this context, regardless of pricing levels, will always be avoided.

The Honorable Henry Waxman

1. **Many have expressed a preference for competitive marketplace forces to discipline companies to implement adequate cyber security measures. Concerns have also been expressed about overly prescriptive approaches to regulation. Given the potentially severe consequences to the country of a significant cyber breach, are there any generally applicable mandates that you believe would be constructive? For example, what if some other company that is part of the Internet ecosystem fails to be as diligent as yours and, as a consequence, causes harm to your network, or even harm to a critical infrastructure sector? Should there by some way of holding all stakeholders accountable for employing best practices?**

Answer: We share the concern that prescriptive government mandates are poorly suited to combat dynamic cyber-threats. The challenges we face in cybersecurity simply cannot be solved by regulation of cybersecurity providers or critical infrastructure and key resource entities that tends to focus on processes rather than results. Such regulation tends to drive up costs, and

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

Response of Edward Amoroso, Ph.D.
Senior Vice President & Chief Security Officer, AT&T
to
June 11, 2012 Additional Questions for the Record of the Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses"

thereby drive down demand, and often does not result in any actual improvement of security. Instead, the best way to address the problem is through private sector innovation and investment, spurred by market demand for more secure products and services. The government can accelerate that demand through education about the need for security—either through self-provisioning or through the purchase of private managed security services.

Threats to our network may occur without regard to the diligence of other entities in the Internet ecosystem, and we don't manage our networks on the assumption that all entities with who we exchange traffic operate according to a set of best practices. Our cybersecurity professionals continuously monitor our global network for safety, security and reliability regardless of the source or destination of the data traversing it.

2. Specifically concerning mobile devices, especially smart phones and tablets, what is the cybersecurity implications of the wide open apps market, and what is the risk of botnets spreading to mobile devices?

Answer: We are seeing the acceleration of cyber threats into the mobile environment, although the overall number of cyber threats targeted to fixed devices remains larger. The emerging mobile applications marketplace is just one aspect of this threat acceleration. While AT&T maintains stringent controls over the mobile applications it develops and distributes through its own mobile applications store, it is unable to exercise control over the broader applications market.

A number of industry groups are now working to address the various security issues in the mobility environment, and minimize the potential impacts of the expanding threats. In particular, as a leader in providing mobility services in the United States, AT&T is now taking steps to provide all of our mobile customers with advanced security protection in their mobile devices and in our network, and to offer our enterprise customers comprehensive security solutions for their business needs, including the ability to securely access their cloud based information and applications from mobile devices. Several traditional software or edge based security firms, offer a range of mobile security solutions including traditional anti-virus and anti-malware options. Additionally, several mobility standards bodies have also established working groups to review security and privacy address consumer awareness.

3. You stressed the need to foster information sharing between the government and private industry as well as among private companies. What protection do you think are necessary to protect civil liberties and consumer privacy? What do you believe

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

Response of Edward Amoroso, Ph.D.
Senior Vice President & Chief Security Officer, AT&T
to
June 11, 2012 Additional Questions for the Record of the Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses"

would be the reasonable boundaries to liability protections, and anti-trust exceptions?

Answer: It is critical that stakeholders fully appreciate that the cyber threat monitoring, activities undertaken by communications network and security providers are, as a rule, limited to non-content metadata, and are undertaken solely to defend network systems and assets against cyber-attack. Typically, cybersecurity algorithms are performed by computers and then often only on metadata, rather than on users' private content. Generalized fears of government or enterprise "monitoring" of private communications content may be inhibiting more rapid adoption of safe and secure cybersecurity practices, which are agnostic to that content, particularly in the enterprise space.

A legal framework that provides clarity with respect to authorized cyber threat monitoring and threat defense activities, as well as the specific types of information about emerging threats that can be shared, with whom it can be shared, and for what purpose, preferably in functional, pragmatic terms that cyber security professionals can understand without the need to resort to legal interpretation, will assure that individual privacy and civil liberties are protected. We believe a defined structure that facilitates both the timely and effective sharing of information and compliance with a simplified legal framework for threat information sharing is essential. Though this structure should be outside of government, to help address concerns of the stakeholders you identify in your question, any oversight mechanism should provide for regular review by Congress. Private sector entities should be given protection from potential criminal and civil liability in order to encourage and facilitate the rapid and widespread adoption of cybersecurity practices, especially if threat information sharing takes place within this framework.

July 11, 2012

The Honorable Greg Walden
Chairman
Subcommittee on Communications and the Internet
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden:

On March 7, I was a witness on behalf of CenturyLink at a hearing before the Subcommittee on Communications and the Internet on "Cybersecurity: The Pivotal Role of Communications Networks." I recently received questions for the record from several Subcommittee members. Please find my responses below, and feel free to contact me for any additional information or clarification.

Sincerely,

R. David Mahon

David Mahon
Vice President & Chief Security Officer
CenturyLink

The Honorable Anna Eshoo

1. **I believe the integrity of the supply chain is essential to the security of our nation's communications networks. Do you share these concerns? If so, what role should the Federal government, including the FCC play to ensure supply chain security?**

   CenturyLink agrees that the integrity of the supply chain is essential and takes numerous measures to test the security and integrity of components going in our network. By extension, this testing becomes one component in establishing which vendors CenturyLink chooses to work with over time.

The federal government already plays a number of important roles in cybersecurity and supply chain risk management, including managing supply chain risks for federal information systems. This supply chain management is especially important when provisioning sensitive government networks through the acquisition processes, which, when appropriate, results in some of these practices being adopted by the private sector. Through its intelligence gathering and other uniquely government-related functions, the federal government is sometimes in a position to identify emerging risks and threat scenarios that private sector companies might not otherwise know about. By maintaining a close partnership with key government agencies, communications providers may be able to learn about these emerging concerns, and better minimize their own supply chain risks.

Through public-private partnerships that the communications industry maintains with the Department of Homeland Security, as our Sector Specific Agency, the government has also increasingly facilitated important information sharing discussions surrounding common approaches to emerging threats.

CenturyLink believes these federal government roles are important and should be continued and further refined to better assist the communications industry with addressing supply chain risk management issues. While CenturyLink has engaged in a number of voluntary cybersecurity initiatives with the Federal Communications Commission (FCC), we have not considered an official role for the FCC on supply chain issues.

2. **How do we ensure private sector commitment to a voluntary ISP code of conduct, like the one being proposed by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC)?**

CenturyLink believes the federal government can ensure private sector commitment by continuing to build trust with private sector partners and working with them to refine best practices as cybersecurity challenges evolve.

CSRIC is a good example of this. CenturyLink actively provided support during the development of the voluntary Anti-Bot Code of Conduct for ISPs (ABC's for ISPs) and the associated industry best practices. In fact, CenturyLink has already voluntarily implemented the ABC's for ISPs and provides notification and education for its customers regarding bot activity and supports efforts to detect and remediate

bots through collaboration with other ISPs. The voluntary nature of the code of conduct is fundamental to its continued success.

The development of the code required cooperative dialogue, among a wide range of communication providers, regarding consumer education, bot detection, consumer notification, and remediation. The voluntary code allows providers the flexibility to take action against bots in a manner that is tailored to their business architecture, technologies, and challenges.

Due to the cooperative nature of the code's development, it has received broad support from major US ISPs. Many ISPs leveraged their code participation during the FBI's recent DNS Changer malware event. This is a clear example of how voluntary public-private partnerships can be utilized to quickly respond to industry issues.

3. **How do service providers avoid using the lowest cost provider of equipment, even if there are risks associated with such a supplier? Is it reasonable to expect them to properly evaluate the supply chain risks associated with an equipment provider?**

Service providers procure network equipment that will best assure the availability, reliability, security and integrity of the services they offer; cost is just one consideration. Service providers actively seek information from various sources to provide insights into these service attributes, and are better positioned to evaluate risks associated with particular equipment and/or providers.

Service providers may benefit from the federal government sharing any of the concerning risks or risk scenarios that they are aware of. A frank, open channel of communication with key government agencies would help service providers better understand and test these concerns. This would be particularly useful if government information associated with a low cost equipment provider, that otherwise meets or exceeds commercial performance standards, is available.

The Honorable Henry Waxman

1. **Many have expressed a preference for competitive marketplace forces to discipline companies to implement adequate cyber security measures. Concerns have also been expressed about overly prescriptive approach to regulation. Given the potentially severe consequences to the country of a significant cyber breach, are there any generally applicable mandates that you believe would be constructive? For example, what if some other company that is part of the Internet ecosystem fails to be as diligent as and, as a consequence, causes harm to your network, or even harm to a critical infrastructure sector? Should there be some way of holding all stakeholders accountable for employing best practices?**

   While CenturyLink cannot speak to other industry sectors, we believe the communications sector has been very responsive to cybersecurity risks and has been committed and constructive partners with the federal government in identifying and taking appropriate measures to protect critical infrastructure. CenturyLink shares the sense of urgency and seriousness that federal policymakers do regarding cyber threats; however, we believe mandates on the communications sector would modify the sector mindset to one of minimal, regulatory compliance in an ever-evolving threat environment, and would ultimately be counterproductive to what has otherwise been a successful partnership.

2. **Specifically concerning mobile devices, especially smart phones and tablets, what are the cybersecurity implications of the wide open apps market, and what is the risk of botnets spreading to mobile devices?**

   While CenturyLink does not offer retail mobile service, we recognize that botnets are a potential threat in both the wireline and wireless markets. We believe that a mix of cooperation with law enforcement, information sharing, consumer education, and various technical measures could be employed to address the threat in both sectors.

House Subcommittee on Communications and Technology
"Cybersecurity: The Pivotal Role of Communications Networks"
March 7, 2012
Responses of John Olsen, Senior Vice President and Chief Information Officer of MetroPCS Communications, Inc., to Additional Questions for the Record

Questions from the Honorable Anna Eshoo

1. I believe that the integrity of the supply chain is essential to the security of our nation's communications networks. Do you share these concerns? If so, what role should the Federal government, including the FCC play to ensure supply chain security?

Yes. However, MetroPCS does not believe that additional regulation is required or warranted at this time, particularly for wireless providers that do not provide services to the government, local public safety organizations or utilities. Wireless services at the retail level are competitive and wireless providers are already well incented to protect their networks and their customers, and this is particularly true for month to month service providers, like MetroPCS. If we do not provide the level of protection our customers want or demand, they can terminate service without penalty and activate service with a competitor. However, if the Federal government decides it needs to do something in this area, one suggestion may be for the FCC to require all equipment manufacturers to annually audit and certify that the integrity of their supply chain is secure as part of the FCC equipment authorization process. This would be similar to the certifications required under Sections 302 and 902 of the Sarbanes-Oxley Act of 2002.

2. How do we ensure private sector commitment to a voluntary ISP code of conduct, like the one being proposed by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC)?

MetroPCS is aware of the voluntary ISP codes of conduct like the ones proposed by the FCC's CSRIC advisory group. It is important that private sector providers, like MetroPCS, have the flexibility to defend their networks without giving away their playbooks to potential cyber attackers and without being forced to follow a one-size-fits-all plan that is developed to accommodate the business plans of our larger competitors. In that light, it is important that codes of conduct are voluntary and not mandated. Nonetheless, many of the nation's largest wireline and wireless ISPs (many of whom provide services to government, public safety, utility and business entities) have publicly committed to the codes of conduct, and MetroPCS already follows many industry standards and best practices and may utilize many of the concepts in the ISP codes of conduct that are relevant to our security strategy, network design and business model. Given the retail competition for wireless services and the voluntary adoption already by industry of these codes of conduct, MetroPCS does not believe that such codes of conduct therefore need to be mandated.

3. How do service providers avoid using the lowest cost provider of equipment, even if there are risks associated with such a supplier? Is it reasonable to expect them to properly evaluate the supply chain risks associated with an equipment provider?

As noted above, MetroPCS shares the concern of the Committee about supply chain security. To mitigate the risk, we avoid using in most instances the same vendor for infrastructure and for customer equipment. We also use reputable vendors with a proven track record. For example, our communications networks use four well known and established network vendors – such as Alcatel Lucent, Ericsson, Cisco and Samsung. We also purchase handsets and smartphones from well-known and established vendors. The operating system used on the smartphones is licensed directly to the manufacturer by Google. Because our handset and smartphone vendors are not our primary communications network vendors, it mitigates the risk that an embedded handset and smartphone threat is able to exploit vulnerabilities in our network. Further, MetroPCS does not provide services to the government, local public safety organizations or utilities. Given that our business model is based on month to month service, we are well incented to protect to our networks and our customers. If we do not provide the level of protection our customers want or demand, they can terminate service without penalty and activate service with a competitor. Further, the lowest priced competitor does not always pose a substantial supply chain risk. In many cases, the market for this equipment is competitive. As such, the supplier with the highest supply chain risk in all instances may not be the lowest priced supplier.

Questions from the Honorable Henry Waxman

1. Many have expressed a preference for competitive marketplace forces to discipline companies to implement adequate cyber security measures. Concerns have also been expressed about overly prescriptive approaches to regulation. Given the potentially severe consequences to the country of a significant cyber breach, are there any generally applicable mandates that you believe would be constructive? For example, what if some other company that is part of the Internet ecosystem fails to be as diligent as yours and, as a consequence, causes harm to your network, or even harm to a critical infrastructure sector? Should there be some way of holding all stakeholders accountable for employing best practices?

We do believe that market forces are better suited to respond to constantly changing cyber threats. If regulations are considered, MetroPCS urges that the requirements be flexible and tailored to the size of the threat. Not all networks pose the same risk to the larger Internet ecosystem and critical infrastructure. It is important that private sector providers, like MetroPCS, have the flexibility to defend their networks without giving away their playbooks to potential cyber attackers and without being forced to follow a one-size-fits-all plan that is developed to accommodate the business plans of our larger competitors. Regulatory compliance and costs can be particularly burdensome for providers who compete by providing an affordably

priced, differentiated service for consumers. For example, carriers like Verizon, which is the largest provider of communications services to the U.S. government and also provides services to public safety entities and businesses (e.g., critical infrastructure), can easily shift the cost of complying with new regulations back on its government, public safety and business customers. On the other hand, MetroPCS, which does not provide services to the U.S. government, public safety or other critical infrastructure, would be forced to increase its rates on its individual customers to cover the compliance costs if faced with the same regulatory mandates as Verizon. MetroPCS does follow many industry standards and best practices that are relevant to our security strategy, network design and business model. However, the best practices for MetroPCS – and our risk to the larger Internet ecosystem – are not the same as Verizon's. Further, where feasible, MetroPCS includes provisions in its agreements with suppliers and vendors requiring them to not introduce malicious or other threats to cybersecurity into any network connected to MetroPCS.

2. Specifically concerning mobile devices, especially smart phones and tablets, what are the cybersecurity implications of the wide open apps market, and what is the risk of botnets spreading to mobile devices?

The operating systems on the smartphones that MetroPCS offers to customers are licensed directly to the manufacturer by Google. MetroPCS and smartphone owners must depend on Google to determine whether its operating system contains any security vulnerabilities. Further, it has been an objective of many members of the Subcommittee for wireless providers to allow customers to bring and place in service their own compatible smartphones on their networks. MetroPCS allows this, but it makes it even more difficult for MetroPCS to have any visibility into any vulnerabilities which a particular smartphone operating system may have. And while MetroPCS operates a limited application store, its users also have access to the Google Marketplace, which contains hundreds of thousands of applications. MetroPCS does not have the resources nor the ability to police the Google Marketplace and prevent malicious applications. Just like a PC or Mac owner, it is the responsibility of the smartphone owner to download all security patches, to load security software and to not download any applications which may have security vulnerabilities.

3. Your testimony focused mainly on the security of your company's internal systems, but would you please discuss how you address the security concerns for the smart phone devices and associated operating systems that use your network? What level of network access do outside partners have?

Our communications networks use four well known and established network vendors – Alcatel Lucent, Ericsson, Cisco and Samsung. We also purchase smartphones from well-known and established vendors, and the operating system used on the smartphones is licensed directly to the manufacturer by Google. Because our smartphone vendors are not our primary communications network vendors, it mitigates the risk that an embedded handset and smartphone threat is able to

exploit vulnerabilities in our network. Issues regarding the Google operating system are addressed in the response to question 2 above. Accordingly, smartphone vendors and the smartphone operating system vendors have no or limited access to our communications networks.

Scott Totzke
Senior Vice President, BlackBerry Security Group
Research In Motion
Answers to Questions for the Record

The Honorable Anna Eshoo

1. **I believe that the integrity of the supply chain is essential to the security of our nation's communications networks. Do you share these concerns? If so, what role should the Federal government, including the FCC play to ensure supply chain security?**

   Research In Motion considers the security of the supply chain integral to the development and release of secure products. This is why we have cryptographic authentication and authorization challenges built directly into our hardware and into the processes required to manufacture that hardware, so that no matter where a device is manufactured there is a consistent level of security embedded in the end product. The federal government should promote information sharing so that companies responsible for hardware manufacturing can correct or dispel suspected supply chain problems/safety breaches, and provide public education about what a secure supply chain entails.

2. **How do we ensure private sector commitment to a voluntary ISP code of conduct, like the one being proposed by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC)?**

   Research In Motion is not an ISP in the United States.

3. **In your testimony, you advocated for "security testing and certification that establishes a baseline for technology vendors." Should this baseline be established by industry, government or some collaboration between the two?**

   The responsibility lies with vendors to develop and release mobile devices that provide the level of security required by the people who use them. The functionality of mobile devices is developing rapidly, and vendors need to prioritize innovation while providing assurance of product security to governments and customers, as well as educating users about the security level of which they can be assured with use of the device. The value of consistent application of government-validated standards across the mobile industry is to provide users better protection by preventing them from choosing a less secure solution without understanding the risk to their personal and professional information.

   The functionality of mobile devices should therefore comply with the standards put in place by the U.S. Government's National Institute of Standards and Technology (NIST). Greater adherence by all vendors to trusted validation programs like FIPS and any new technology

neutral standards will help communicate levels of security in straightforward terms and allow users to make informed purchasing decisions.

The Honorable Henry Waxman

1. **Many have expressed a preference for competitive marketplace forces to discipline companies to implement adequate cyber security measures. Concerns have also been expressed about overly prescriptive approaches to regulation. Given the potentially severe consequences to the country of a significant cyber breach, are there any generally applicable mandates that you believe would be constructive? For example, what if some other company that is part of the Internet ecosystem fails to be as diligent as yours and, as a consequence, causes harm to your network, or even harm to a critical infrastructure sector? Should there be some way of holding all stakeholders accountable for employing best practices?**

   There are many state and federal laws and regulations currently enacted that encourage industry to vigilantly guard against cyber threats. These include threats of litigation by shareholders, enforcement under the varying state data breach laws, the fiduciary responsibilities of management and federal securities laws, and sector specific regulations, including the communications sector, to name a few. Broad sectors of the government, such as the Department of Defense, have standardized governance models for minimum security capabilities that vendors must adhere to such as those outlined in Homeland Security Presidential Directive 12. These types of initiatives drive industry to consciously deliver products that meet a consistent level of security if they wish to sell the government agencies.

2. **Specifically concerning mobile devices, especially smart phones and tablets, what are the cyber security implications of the wide open apps market, and what is the risk of botnets spreading to mobile devices?**

   Mobile devices are becoming a more attractive target for attackers, and attacks are becoming increasingly focused on the end user's personal information. Mobile devices really need to be viewed in the same category as any other computer systems as they can now store and access a vast amount of personal information, including financial details. The ability of many smartphones to allow users to install apps from trusted and untrusted sources introduces further risk that personal data on mobile devices may be used maliciously. Once installed, third-party apps, if not carefully vetted by the user, may take advantage of permissions to use the wide range of additional communication and connection features smartphones support, like SMS and social networking applications. The relatively limited display mechanisms available to communicate critical information to the user and the trust that may inherently be applied to a given application storefront may prevent the user from understanding what the app is accessing on the smartphone with or without their explicit consent.

   The greater the capabilities of smartphones and tablets, the more likely they are to be susceptible to the same security risks as PCs. A computer typically becomes a bot within a botnet (a collection of infected computers that has been taken over by an individual) when it

downloads a malicious file or an email attachment that has malware embedded, or through exploitation of a software vulnerability. Mobile botnets function in much the same way as PC botnets, through a command and control structure that transfers commands from the controlling individual to the infected system and then receives a data response back. This data transfer may occur using any communication avenue available to the infected system (HTTP, IRC, instant messaging clients, and, on mobile platforms, SMS), many of which are now equally available to mobile device as to PCs.

In many ways, we can expect mobile security to mirror what was witnessed over the last decade for desktop and server based systems as attackers will attempt to exploit any potential weaknesses in these relatively new mobile platforms. We are starting to see the focus of the security research community shifting from traditional computing platforms to mobile platforms as devices have grown in popularity and in many cases represent the first, and often only, connection to the Internet for the user. This shift in research places an increasing importance on mobile device makers to develop and maintain industry leading security features and configuration options to help mitigate these evolving threats. Additionally, it will become increasingly necessary for security to be considered in all phases of application development to ensure that resiliency against attacks is built into mobile devices from the start.