AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND PRIVATE SECTOR RESPONSES

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 8, 2012

Serial No. 112–112

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

U.S. GOVERNMENT PRINTING OFFICE
82–628 PDF WASHINGTON : 2014

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 *(ex officio)*
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. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	7
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachusetts, opening statement	8
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	8
Prepared statement	10
Hon. Lee Terry, a Representative in Congress from the State of Nebraska, opening statement	12
Hon. Mike Rogers, a Representative in Congress from the State of Michigan, opening statement	12
Hon. Doris O. Matsui, a Representative in Congress from the State of California, opening statement	13
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, prepared statement	114
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, prepared statement	115
WITNESSES	
Bill Conner, President and Chief Executive Officer, Entrust	14
Prepared statement	17
Answers to submitted questions	119
Robert B. Dix, Jr., Vice President, Government Affairs and Critical Infrastructure Protection, Juniper Networks	26
Prepared statement	29
Answers to submitted questions	127
James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies	42
Prepared statement	44
Answers to submitted questions [1]	
Larry Clinton, President and Chief Executive Officer, Internet Security Alliance	51
Prepared statement	53
Answers to submitted questions [2]	136
Phyllis Schneck, Vice President and Chief Technology Officer, Public Sector, McAfee, Inc.	73
Prepared statement	76
Answers to submitted questions	210
SUBMITTED MATERIAL	
Majority memorandum	116

[1] Mr. Lewis did not answer submitted questions for the record by the time of printing.

[2] Additional information provided by Mr. Clinton and referenced on page 141 is available at http://www.verizonbusiness.com/resources/reports/rp__data-breach-investigations-report-2011__en__xg.pdf.

CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND PRIVATE SECTOR RESPONSES

WEDNESDAY, FEBRUARY 8, 2012

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

The subcommittee met, pursuant to call, at 9:39 a.m., in room 2322 of the Rayburn House Office Building, Hon. Greg Walden (chairman of the subcommittee) presiding.

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

Staff present: Carl Anderson, Counsel, Oversight; Gary Andres, Staff Director; 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; David Redl, Counsel, Communications and Technology; Jeff Cohen, Democratic FCC Detailee; Kara Van Stralen, Democratic Special Assistant; Shawn Chang, Democratic Chief Counsel, Communications and Technology; and Roger Sherman, Democratic Chief Counsel, Energy and Commerce.

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

Mr. WALDEN. I am going to call the order the Subcommittee on Communications and Technology. I want to welcome our members and our witnesses for today's hearing on cybersecurity threats to communications networks and private sector responses.

Back in October, the House Republican Cybersecurity Task Force recommended that the committees of jurisdiction review cybersecurity issues. So this hearing continues our committee's review of cybersecurity issues with an examination of threats to communications networks and the responses of the private sector. Threats to communications networks have come a long way in a very short time and they are very, very real and serious.

Before coming to Congress, I spent about 22 years as a radio broadcaster. And as a small businessman, I had to worry about securing our communications network, and back then, 20 years ago, it was relatively straightforward. You had to have a fence around the tower and you couldn't let people get near the transmitter and

a few things like that. And every once in a while somebody would come and shoot an insulator out or something and you kind of got grumpy and had to repair that, and every once in a while some idiot would try to cut the guy wires, and those usually spun around and got them. That never happened at my stations, but it does happen occasionally. But all of that was sort of security of that wireless age. Not anymore.

While physical security remains important, cybersecurity has also become a pressing concern. Now a small business confronts a dizzying array of threats online from the Zeus Trojan horse to Stuxnet, from LulzSec to botnets. These threats are serious. Unless our cyber defenses hold, a bad actor could drain the bank account of a business, crash an online company's Web site, or launch a barrage of cyber attacks on a company's network. Those are serious consequences for any business, and especially for the small businesses that are at the heart of creating new jobs in this economy. And indeed, in our small business, I don't know, 10 years or so ago when we did create a computer network and put everything up on digital audio, our main server was hacked and taken over, and all of a sudden it started running slower and slower and slower and eventually we determined it had been overtaken.

Every month, we learn more about these cyber threats, and what we have learned thus far is of great concern. I am concerned that our communications networks are under siege. I am worried that the devices consumers use to access those networks are vulnerable, and I am concerned that our process for looking at communications supply chain issues lacks coordination. I am also concerned that our cyber defenses are not keeping pace with the cyber threats.

Now, in this hearing, we are lucky to have the voices of five private sector witnesses to guide us through the complex issue of cybersecurity. I am hoping that you will tell me that cyberspace is secure and we can all rest easy at night. Unfortunately, I have read your testimony and it is not so. So I expect that you will tell us that the threats to our communications networks are all too real, American businesses are losing dollars, jobs, intellectual property and much, much more because of cyber crime and cyber espionage, and that our national security is potentially at risk as well.

I also expect that you will explain what the private sector is doing to fortify our cybersecurity defenses. The private sector owns most of the critical infrastructure—the wires, the servers, the towers and base stations—that make up our communications networks, and they are on the front lines of cybersecurity. So I want to know what cybersecurity services are being offered to consumers, what protections are being deployed in our communications networks, and what affirmative steps the private sector has taken to lock down the supply chain and to combat cyber crime.

I also expect to hear what you think the appropriate—and underscore "appropriate"—the Federal role is. Are Federal laws and regulations helping or interfering with information sharing? Are Federal regulations of cybersecurity practices appropriate, and if so, how? Should the Federal Government be providing incentives for Internet service providers and other members of the private sector to invest and innovate in the cybersecurity arena? And how should our country's fiscal state shape our discussion of the Federal role?

These questions and others will form the basis for deciding what cybersecurity legislation, if any, is needed in the near term, and how we can best secure cyberspace in the long run. So I want to thank the panelists today for taking time out of your schedules to be here to help inform this important subcommittee and the Energy and Commerce Committee on what we should do and how we can be better informed in doing our job.

[The prepared statement of Mr. Walden follows:]

Statement of the Honorable Greg Walden

Chairman, Subcommittee on Communications and Technology

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

February 8, 2012

Back in October, the *House Republican Cybersecurity Task Force* recommended that the committees of jurisdiction review cybersecurity issues. This hearing continues our Committee's review of cybersecurity issues with an examination of threats to communications networks and the responses of the private sector.

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, and back then it was relatively straightforward. Maybe you bought a fence to surround your broadcast tower. Maybe you hired a security guard to watch your station at night. But physical security was the concern.

Not anymore. While physical security remains important, cybersecurity has also become a pressing concern. Now a small business confronts a dizzying array of threats online from the Zeus ("zoose") trojan horse to Stuxnet ("stucks-net"),

from lulzsec ("lulls-seck") to botnets. These threats are serious. Unless our cyberdefenses hold, a bad actor could drain the bank account of a business, crash an online company's website, or launch a barrage of cyberattacks on a company's network. Those are serious consequences for any business, and especially for the small businesses that are at the heart of creating new jobs in our economy.

Every month, we learn more about these cyberthreats. And what we have learned thus far worries me. I am worried that our communications networks are under siege. I am worried that the devices consumers use to access those networks are vulnerable. I am worried that our process for looking at communications supply chain issues lacks coordination. And I am worried that our cyberdefenses are not keeping pace with the cyberthreats.

In this hearing, we are lucky to have the voices of five private-sector witnesses to guide us through the complex issue of cybersecurity. I am hoping that you will tell me that cyberspace is secure. Unfortunately, I expect that you will tell us that the threats to our communications networks are all too real and that American businesses are losing dollars and jobs because of cybercrime and cyberespionage, and that our national security is potentially at risk, as well.

I also expect that you will explain what the private sector is doing to fortify our cyberdefenses. The private sector owns most of the critical infrastructure—the wires, the servers, the towers and base stations—that make up our communications

networks, and they are on the front lines of cybersecurity. I want to know what cybersecurity services are being offered to consumers, what protections are being deployed in our communications networks, and what affirmative steps the private sector has taken to lock down the supply chain and to combat cybercrime.

I also expect to hear what you think the appropriate role of the federal government is. Are federal laws and regulations helping or interfering with information sharing? Are federal regulations of cybersecurity practices appropriate? Should the federal government be providing incentives for Internet service providers and other members of the private sector to invest and innovate in the cybersecurity arena? And how should our country's fiscal state shape our discussion of the federal role?

These questions and others will form the basis for deciding what cybersecurity legislation, if any, is needed in the near term, and how we can best secure cyberspace in the long run. I thank the panelists for their testimony today, and I look forward to a lively discussion of these issues.

Mr. WALDEN. With that, I would recognize the gentlelady from California, the ranking member of the subcommittee, 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, for convening this morning's important hearing, and I want to welcome the witnesses and I am especially pleased that Juniper Networks and McAfee, two outstanding Silicon Valley companies, are here to talk to us about tackling the challenges of cybersecurity this morning.

We all recognize the serious threat to our Nation's communications networks. Since 2006, the number of Federal cybersecurity incidents reported to the Department of Homeland Security has increased by 659 percent. That is a whopping number. And the economic impact of these incidents is equally significant. A recent study by the Ponemon Institute estimated that the median annualized cost of cyber crime to a victim organization is $5.9 million per year, an increase of 56 percent from 2010.

The more we rely on the Internet to conduct our business, the more vulnerabilities we create for hackers to exploit. Having served as a member of the House Intelligence Committee for 8 years, I am very well aware of the threat, not just from criminal hackers but also obviously from other countries. But talking about the problem is not enough. We need to act, and that requires the help of both the private sector and the Federal Government. The private sector really represents 95 percent of this, the Federal Government the other 5 percent.

One of the first steps to tackling this growing threat is, I think, education and training. Whether at home or in the workplace, every American should understand what they can do to protect themselves against a cyber attack. Improved information sharing is also a key aspect of our Nation's response to cybersecurity. If we are going to ask industry to report cybersecurity incidents to the government, then we need to establish a clear process to do so.

I am pleased to support our colleague Mike Rogers' effort, the Cyber Intelligence Sharing and Protection Act of 2011. That is one of three or four bills in the House. There are least three or four in the Senate as well.

It is also important to recognize the timely alerts to consumers and businesses can be the difference between an isolated cybersecurity incident and one that impacts millions of users. A voluntary ISP code of conduct currently being developed by the FCC is one of the proposed ways to alert consumers when a botnet or other malware infection is discovered.

Today's hearing is a very important opportunity for us to better understand our subcommittee's role in cybersecurity including what role the FCC and NTIA should play in protecting our Nation's communication networks and how the private sector and other Federal agencies should interact with them.

So thank you to all of the witnesses, those that come from Silicon Valley to instruct us, and with what remaining time I have I would like to yield to Mr. Markey.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. I thank the gentlelady.

Last week, FBI Director Robert Mueller testified that cyber threats will soon surpass terrorism as the number one threat facing the United States. We know from the Department of Homeland Security that there have already been threats to the utility sector. We also know that Russia and China have probed our electricity grid to find vulnerabilities.

Our economy hinges on a reliable flow of power with losses that go into the billions of dollars with every major blackout. Our national security also depends upon it since 99 percent of the electricity used to power our military facilities including critical strategic command assets comes from the commercially operated grid.

Last September, I asked all five commissioners from the Federal Energy Regulatory Commission under our jurisdiction to name the number one threat to electricity reliability. All five commissioners agreed, cyber threats are the number one threat to the grid.

In 2009, the full Energy and Commerce Committee unanimously passed the GRID Act, which I authored along with Chairman Upton. That bill gave FERC the authority to quickly issue grid security orders or rules that vulnerabilities or threats have not been adequately addressed by the industry. It was killed in the Senate. All five FERC commissioners also agreed that giving FERC this authority would increase America's ability to secure our electric grid.

With cyber threats growing by the day threatening our security and our economy, it is imperative that this committee pass the GRID Act so that we can move it forward and empower the FERC to move quickly to safeguard the electric grid from cyber threats that are not sufficiently addressed by industry. We should listen to FBI Director Mueller, to the FERC and to the warnings coming from Russia and China. We should pass the GRID Act soon.

I yield back.

Mr. WALDEN. I thank the gentleman for his comments, and we are now going to recognize the chairman emeritus of the committee, Mr. Barton.

Before I do that, I just want to say how important it is to have members who have been so engaged on this, and especially we are blessed to have Anna here, who served on the Intelligence Committee, and Mike Rogers, who chairs it now, and Lee Terry and Mr. Latta and Mr. Murphy, who is not part of the subcommittee but were on the cybersecurity task force the Speaker appointed, so all of that is most helpful as we tackle both of these issues.

I now recognize the gentleman from Texas, Mr. Barton.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Chairman Walden. I thought Mr. Markey was going to say the experts said the biggest threat to our grid was the EPA, but he went a different way with that.

Back in 2006, Subcommittee Chairman Upton held a hearing on this very same issue, and as full committee chairman, he and I

sent a letter to the GAO asking them to take a look at this issue. The response that we received then is the response that we are receiving today and that is that it is quite possible that we could have a major attack, a cyber attack, in this country that would dramatically affect our country.

According to the Norton cyber crime report for this last year, cyber crime is a $388 billion industry with 431 million adults experiencing at least one cyber crime in the last year. In another study, research has showed that the median annualized cost of cyber crime for companies is over $6 million a year with the range being between $1.5 million to $36 million per year. Now, these are real numbers, real statistics and that is for the year 2011.

As we use the Internet more and more every day, it is absolutely imperative, Mr. Chairman and Ranking Member Eshoo, that we really take this seriously, and as you have pointed out and Anna has pointed out, it is good to have the chairman of the Select Committee on Intelligence on this subcommittee because he has access to information that could be useful if and when we decide to legislate.

So thank you, Mr. Chairman, for holding the hearing. As you know, there is an EPA hearing downstairs in the energy subcommittee, so I will be shuttling back and forth.

[The prepared statement of Mr. Barton follows:]

Opening Statement of the Honorable Joe Barton
Chairman Emeritus, Committee on Energy and Commerce
Subcommittee on Communications, Technology, and the Internet
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses"
February 8, 2012

During my time on this committee, we have discussed the general topic of what the government and private sector should be doing to prevent and mitigate attacks on our Internet infrastructure. As Chairman, I sent a letter to the Government Accountability Office (GAO) requesting a report on our preparedness for a major Internet disruption. The response I received in 2006 is very similar to the response from the GAO today: this country would indeed struggle with addressing such a feat.

According to a Norton Cyber Crime Report for 2011, cybercrime is a $388 billion industry with 431 million adults experiencing a cybercrime in the last year.[1] Also in a study conducted by the Ponemon Institute, research showed that the median annualized cost of cybercrime for the companies involved in the study was at $5.9 million per year with a range of $1.5 million to $36 million each year per

[1] Cybercrime Report 2011. (2011). Retrieved February 7, 2012, from http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

company.[2] These statistics are extremely alarming to me, and it is clear that we must have mechanisms in place to protect our internet.

More Americans are using the Internet daily, and more businesses are using online models to provide convenience to consumers. Like I have said before, protecting our Internet infrastructure is not simply a goal this country should aim to meet, it is an imperative that the United States must achieve. I look forward to hearing from our witnesses.

[2] Ponemon Institute. (2011, August). *Second annual cost of cyber crime study.* Retrieved February 7, 2012, from http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

Mr. WALDEN. Mr. Chairman, if you don't mind yielding to Mr. Terry?

Mr. BARTON. I will yield 2 minutes.

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

Mr. TERRY. Thank you, Mr. Barton and Mr. Chairman.

This is an extremely important hearing and that we have to elevate the level of discussion and potential solutions.

There is only one silver bullet that exists to prevent cyber crimes. That is to completely disconnect your computer from any network. Use it as a paperweight. Maybe just play solitaire. That is it. If you are going to engage in any level of commerce using the Internet, you are at risk, and the only thing we can do is to try to minimize it. There is no silver bullet.

Why these folks are here today is for us to understand what tools may be available. In the cyber task force, one of the things that we concluded is that the vast majority of everyday hacking can be maybe not prevented but go a long way which is basic security features offered by private sector today or the networks or ISPs. But we have to have people to actually purchase those or use those tools. In fact, there was one incident in Omaha with our entity that controls our facilities that never thought that it was important to have those type of securities, and guess what? They were hacked and all of their information was stolen.

But then the next level is where it gets dicey. How do you protect people? How do they protect their data? We can't engage in setting the standards because frankly we set the standards. Before the ink is dry on the bill, the standards have changed.

So you are here to help us understand what solutions may be available to minimize and help secure our infrastructure, and I want to thank you all for being here today. Does anybody else want 48 seconds?

Mr. WALDEN. Mr. Rogers.

OPENING STATEMENT OF HON. MIKE ROGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. ROGERS. Thank you very much. In the short time that we have, I can't tell you a more important issue.

There are a lot of things that can keep you up, as the chairman of the Intelligence Committee, and this one is one of the main ones. Eighty percent of the attacks that happen every day can be prevented by the operator. It is those other 20 percent that are the devil in the details. Between criminal attacks, economic espionage, disruption or attacking, as we would call it, on cybersecurity, we have a very real and present danger when it comes to cyber threats to our networks.

Nobody is more integrated than the United States, and therefore we are more at risk than other countries. I do believe it is unprecedented in history that such a massive and sustained intelligence effort by a government to blatantly steal commercial data and intellectual property to use against the United States is well underway. We don't talk about it a lot because companies are reluctant to talk about it. The real number we think is closer to somewhere between

$300 billion and $1 trillion in lost intellectual property per year. Countries like China are leading that charge. Russia is not far behind. Iran's capabilities are getting better, and the most concerning are non-nation states who are developing cyber capability to conduct disruption and attack activities against targets like the United States. All are serious problems.

I want to thank Anna Eshoo. We did a seminar out at Stanford University on this very issue. I think it was well received. Her support of this bill is incredibly important. I look forward to hearing from the witnesses, and I appreciate you being here so that we can get to that next step and actually do something that helps us have a fighting chance against these cyber threats.

I yield back, Mr. Chairman.

Mr. WALDEN. The chair recognizes the gentlelady from California, Ms. Matsui, who is going to control Mr. Waxman's time.

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

Ms. MATSUI. Thank you very much, Mr. Chairman, for holding today's hearing, and I would also like to welcome our witnesses here today and look forward to your testimony.

There is no doubt that cyber attacks are real and continue to pose significant threats to several aspects of our economy. Communications networks are one of many areas that our Nation must protect and assure safety and soundness, particularly as we consider deploying an advanced nationwide broadband network for public safety. Advanced IP-based technologies and public safety communications heighten the concerns for cybersecurity. This new network, however, will share many of the same cyber concerns as any other network. This is something we have to take seriously and must protect.

Moreover, our economy continues to experience ever-evolving ingenuity and innovation in the American technology industry. One of those technologies which will continue to play a prominent role in our economy, both in the public and private sector, is cloud computing. We are also seeing consumer cloud applications like the iCloud. As I see it, one of the key issues is the challenge of cybersecurity relating to the cloud.

The challenge is to find the critical balance of continuing to foster American innovation and growth while combating cyber attacks. For the most part, the private sector will need to be up to the challenge of managing itself and its networks from potential cyber attacks. That said, I do believe that some balance may be appropriate where the government must work together in partnership with the private sector on enhancing our Nation's cybersecurity preparedness. Simply put, one cannot do it without the other.

Small businesses, many of whom rely on the broadband economy, are also very susceptible to cyber attacks. In many instances, small businesses cannot fend off such attacks because they do not have a plan or lack the resources. Such an attack, though, would be very costly to their businesses. During this economic recovery, the last thing small business owners in my district and across the country

need to worry about is a cyber attack that will hinder their business.

I am pleased that the FCC recently launched a public-private partnership, the Small Biz Cyber Planner, which is an online tool that will allow small businesses to create customized cybersecurity plans. It is important that we continue to educate small businesses and the public in general about the risks that cybersecurity poses to small businesses, the government and to our economy as a whole. I also believe a strong public-private partnership is critical to protect against cyber attacks. It is my hope that partnership continues to foster moving forward.

I look forward to exploring appropriate jurisdiction of this committee, given the communications and technology relevance of cybersecurity. I look forward to hearing from the witnesses today and hope that we will have future hearings in this subcommittee so that we can also hear more about the government's efforts to combat cyber attacks.

Again, I thank the chairman for holding today's hearings, and I would be happy to yield to anyone on our side if they would like to. OK. I yield back the balance of my time.

Mr. WALDEN. The gentlelady yields back the balance of her time.

We will now proceed to the witnesses. We have a very distinguished panel. We thank you again for being here today to share the information you have in your testimony, and we are going to start with Mr. Bill Conner, who is the President and Chief Executive Officer of Entrust. Mr. Conner, thanks for your testimony and we look forward to your comments.

STATEMENTS OF BILL CONNER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ENTRUST; ROBERT B. DIX, JR., VICE PRESIDENT, GOVERNMENT AFFAIRS AND CRITICAL INFRASTRUCTURE PROTECTION, JUNIPER NETWORKS; JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; LARRY CLINTON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET SECURITY ALLIANCE; AND PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, PUBLIC SECTOR, MCAFEE, INC.

STATEMENT OF BILL CONNER

Mr. CONNER. Good morning, Mr. Chairman and distinguished members of the subcommittee. It is a privilege and honor to spend a morning here with you out of the cyber warfare game to discuss and educate what is happening below the screen.

I would like to focus my early comments on the arms race on one particular vector of security, and it is called man in the browser. Now, that vector of security is probably the leading cyber stealer in the world today, and it has been around a while and certainly impacts the small and medium business and it is certainly impacting the change and nature of stealing IP and money both at a country state and at an organized-crime state.

Specifically, it is known as Zeus. It is commonly now combined with SpyEye. For those of you don't know, Zeus was the original

man in the browser software. It started out of the Ukraine and Russia. It went under its own merger and acquisition by its lead competitor in the underground world called SpyEye. Their tools and technology were next generation. They merged in the fall of 2010 behind the scenes. As law enforcement started to attack it, the guy took his money and ran, combined it. In February of last year, that new code is out on the market. You can buy it off the Internet and buy it with 24/7 support. So no longer do you have to be intelligent to write the code. You buy it, you pay for the support, and they will help you design your attack vector on which banks, which geographics you want to do.

How does this technology work? It is real simple. It is very complicated. You cannot find it with the traditional software that you have on your desktop, whether it is an antivirus or the operating system looking for it. It is cloaked software that is really targeted at small and medium business because it is targeted for money. This is a for-money game for that. What it basically does, it targets a small or medium business that probably doesn't have the technology or banking understanding with its supplier to understand how to deal with it. How does it work? I am a treasurer at a small business. I go online to my financial institution. I say I want to move $1,000 or $10,000, let us say $10,000, to a supplier. I have an agreement with my local bank to have online bill pay. I type that in. The bank sees that but before the bank sees it, this software wakes up in the browser and changes the payees from one supplier to, let us say, six mules. It changes the dollar amount from $10,000 to $100,000, so what the bank sees is $100,000 going to six people. That bank says guess what, we've got good security, you had to use a password, it is on your IP address in your network and your location. I am going to send it back because I want a one-time passcode, 30-year-old technology that we are trying to apply to the digital world. It sends it back to the controller of your business and says please confirm by putting your passcode that is going to expire in 30 seconds that you authorized this transaction. That software wakes back up, converts that $100,000 back to $10,000, six payers back to one. You type in your passcode, hit enter to send it back, and guess what? That $100,000 is now gone from the bank. You lose it, the bank loses it. Six mules that are going to feed that money back into organized crime around the world are off and running.

Unlike the personal side where I am protected by FDIC, my friends, you are protected as a small or medium business by nothing, the contract you have written, and if you look around this wonderful country of ours, there is no clear case law. There is case law on both sides of this because the banks said I did nothing. We have had cases overturned that even though a business had only done four transactions in the last year and 20 transactions happened in six hours totaling $2 million when online was only $500,000, that is what is happening.

The good thing is, the technology exists to deal with that today. The banks aren't doing it and small businesses don't know what to do. So our belief is very straightforward. Much like quality, there wasn't a lexicon. To deal with cybersecurity, we need a lexicon.

Much like quality, it isn't a one time like year 2000. We need to do it over time. That is why education is critical.

The second thing you must do is have public-private partnership. I co-chair the DHS piece. I can tell you, the legislative laws around this do not work for anybody, and I think you have got to break public-private at different levels from intelligence to the people like me that try to secure the U.S. government and others to energy grids where Department of Energy works with those types of organizations.

And finally, we must take a unified effort in public and private to defend because it is an arms race and it is a pace as we mentioned earlier. Thank you.

[The prepared statement of Mr. Conner follows:]

Testimony of Bill Conner, President and CEO of Entrust

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

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

February 8, 2012

I'm Bill Conner, President and CEO of Entrust, the leader in identity-based security software solutions. On behalf of Entrust, we appreciate the opportunity to testify today.

Entrust is a world leader in securing digital identities and information. As a security software company, we are in the business of protecting our customers — and by extension your constituents — with proven technology solutions that secure digital identities and information. Over 1,200 enterprises and government agencies in more than 50 countries, including the US Department of Treasury, the Department of Justice, Department of State, and numerous Department of Energy nuclear laboratories, rely on Entrust software.

Entrust provides software solutions that protect digital identities through authentication, enforce control policies through advanced content-scanning, and protect information assets through encryption. Our mission is to work with customers to put in place the technologies, policies and procedures necessary to protect digital identities and information against the most sophisticated cybercriminals — whether they originate as external or internal threats.

Hacking for Harm

Experts agree that cybercrime poses a greater threat to the security of nations, corporations and individuals than ever before. In recent years, cybercriminals have moved from hacking for honor — such as for bragging rights within the hacker community — to hacking for harm and profit; in short, it's now overt criminal activity. Increasingly, the most common victims of targeted cybercrimes are those who can least afford a major financial hit such as small businesses. With the increased dependence of the Internet to conduct business, it is no surprise that cybercrimes — ranging from identity theft to financial fraud to cyber terrorism — have dramatically increased against small and large enterprises. Unlike citizens, who are protected by FDIC regulations, businesses' cash or intellectual property is not safeguarded by law.

Online Security — The Ongoing Effort

At Entrust, we are working around the world with small and large enterprises, governments and law enforcement agencies to enable security software for the good guys. We do this knowing that the total cost to deploy security is dwarfed by the cost of what is at stake. Cybersecurity is

similar — a quality-control process in that it must be disciplined, measured and continually improved upon on a daily basis. The challenge I face at the helm of Entrust is to make this possible for companies and governments in a cost-effective and uncomplicated way.

Underlying our efforts is a fundamental belief that success does not mean entities lock down their data. What it should mean to you as policy makers is that they appropriately secure their data so that the benefits of online and digital activity are not impaired, while confidence in the security of the network is maintained.

In short, if you have the image in your mind that a successful cybersecurity strategy is a moat, your strategies, laws and regulations will fail. A moat does not protect from attacks from within, which constitute nearly 80 percent of all cybercrimes. Putting all your faith in a moat also fails to adapt to new threats that defeat such an impoundment and results in data being locked down, which undermines the entire benefit of the digital economy.

The good news is that I have the opportunity to work with many of my peers in coordinating strategies to enhance the positive aspects of the Internet's promise and to combat those who abuse and attack it. There are strategies out there today that work.

But we must be ever-vigilant as cybercriminals continue to outpace our gains with new tricks and technology of their own. That is why we must fight this on a national level and involve the government, enterprises and citizens.

No one is immune. Last year alone, we saw numerous high-profile attacks ranging from Northrop Grumman to Lockheed Martin even to security companies like EMC/RSA, Comodo, Symantec and VeriSign being victims of breaches. Sophisticated attacks such as these are clear evidence that organizations need greater layered security to thwart today's savvy cyber terrorists. Our industry must be proactive in developing solutions that empower organizations to quickly respond to attacks without compromising day-to-day operations. It is also apparent that, as a nation, we are not doing enough to protect our assets and personal information.

The Zone Defense

Sadly, the football season is officially over. However, it seems to me that cyber defense is much like playing defense in football — you don't know what play the other team is calling, therefore, you need to defend against everyone. We first need to understand what offensive strategy we are up against. If the offense sees a hole in your front line, they will exploit it. If they see you are exposed in the secondary, they will attack there. And they will keep trying new angles until you react to shut down that vulnerability.

Cyber security is much the same way — businesses do not know how they will be attacked. They don't know if the threat comes due to a download from an employee surfing the Web, via an attack from within, or from a virus that may have entered the system on an email. What we

do know is, that to win, large government and private organizations of all sizes need to have a strategy to deal with the range of threats. If we wait until we are hacked, it's too late.

Cybercriminals will search for that open door and if they find it, they will wreak havoc on data and possibly divert a company's payments or IP to the bad guys. Consider the amount of time and money it takes a company that has lost all its data to a cyber-attack — not to mention the significant hit to the credibility they lose with their customers if a cybercriminal stole personal information.

Let's be clear. What we face is a threatening cyber environment where warfare is being conducted by foreign governments, international crime rings and common thieves in the U.S. It takes everyone — government, major organizations, small businesses and individuals — working together to defeat those forces.

Moore's Law

To put this all in context, hardware technology follows Moore's Law, which states that capacity doubles and cost halves every 18 months. In the new cyber world, software tools are changing in days, not years, and in many cases hours or even minutes. That makes it a constant real-time battle for all of us.

We are facing a wide range of extremely dangerous enemies armed with expensive and sophisticated hardware, software and boldness. They function in an environment where their white-collar crime, even if identified and apprehended, brings only minimal punishment. This is because most of these attacks are across sovereign borders around the globe.

The good news is that technology and solutions exist today to thwart these cybercriminals. However, it must be applied consistently and universally to deny cybercriminals the easy access they have today.

Shortcomings of FFIEC Guidelines

Let me give you a specific example. The Federal Financial Institutions Examination Council (FFIEC) recently updated its guidance for financial institutions offering Internet-based products and services. Unfortunately, these guidelines only hit at the minimum level of security and are already outdated.

Just like the guidance they released in 2005, the guidelines do not place accountability for implementation nor do they mandate any specified timeframe. This puts consumers and businesses at risk when they conduct business online with their bank. And worse yet, it gives the false impression to consumers and the marketplace that entities are safe when, in reality, they are barely doing anything at all.

Even more alarming, the updated FFIEC regulations do nothing to help small- and medium-sized businesses. So while the guidance falls short of protecting larger financial institutions, it's also all but ignoring the organizations that may need the most legal protection.

Diagramming Advanced Malware

With that in mind, here is one example of a real-world threat that we have encountered that has not received as much attention as data breaches. It is, however, one of the biggest cybercrimes and threats today. The threat is called ZeuS or SpyEye, which is a "man-in-the-browser" malware that targets mid- to small-sized companies. This is a threat you and your constituents need to be aware of and concerned about.

The problem arises when someone within an organization is surfing the Web and accidentally installs software that opens a door for criminals. The software may install when an employee has visited a legitimate website, but one that has unknowingly become infected, or they may have simply clicked the red "x" to close a pop-up ad or notification thinking that all they were doing was shutting down the ad.

In reality, that click prompts the malware to install on their system and then promptly hides itself. In fact, once the malware is installed it is extremely difficult to detect. The malware is crafted to avoid detection by antivirus tools that you all know and probably use.

This malware sits dormant, waiting for someone on the system to log in to a corporate bank account online. When it sees that bank URL pass by, it wakes up and begins to intervene transparently in whatever transaction is being conducted.

Let me explain how it works.

- A consumer, or more likely an accountant, in a small business initiates an online payment to their local utility for $1,000.
- The malware on a PC, laptop or tablet sees the bank URL and online payment. It then "wakes up" and translates that payment into, let's say, six different transactions totaling $100,000 going to six individual accounts.
- The bank then receives the request for these six transactions totaling $100,000 and asks the accountant to confirm the transactions by entering a one-time passcode (OTP) to authenticate the transactions.
- The malware intercepts this request and re-translates the six transactions back to the original single transaction for $1,000.
- The accountant, therefore, sees the original request for the utility to be paid $1,000 and is asked by the bank to enter their specific one-time passcode.

- The controller then enters a one-time passcode to authenticate the transaction and sends it back to the bank.
- Unfortunately, the malware accepts the one-time passcode and again re-translates the single $1,000 transaction to the six transactions totaling $100,000.
- The bank then believes it is a set of authorized corporate transactions based on the passcode the client provided and executes those transactions for $100,000.
- Now both the small business and the bank are missing $100,000.

This is the kind of threat that can and does happen in every state, every day. And not just at multinational companies. It can and does happen to smaller enterprises that aren't as sophisticated in how to protect themselves nor consider themselves to be a target of multinational crime schemes. But they are wrong. This has and does happen to businesses that populate Main Street in every state.

Malware Hitting Home

Let me give you a real-life example. Plano, Texas-based Hilary Machinery, one of the largest machine tool distributor service organizations in the southwest, had $800,000 drained from its bank accounts in two days. It wasn't the company's financial institution that discovered the error. It was Hilary Machinery itself.

Between November 9-10, 2009, PlainsCapital Bank received fraudulent wire-transfer instructions from a group that infiltrated the bank accounts of Hilary Machinery. Some of the transfers involved sums in excess of $100,000, while others were as small as $2,500. Each transfer was made to a different account, which was highly unusual, and outside the norm for the company. PlainsCapital Bank was able to recover all but approximately $200,000 of the lost funds.

Now, who is responsible for the loss was a matter of question. Hilary Machinery believed that PlainsCapital should have been held liable, sued the bank and demanded repayment of the remaining $200,000.

In turn, PlainsCapital counter-sued, saying their security was, in fact, reasonable by industry standards and that it processed the wire transfers in good faith. The lawsuit was eventually settled, but the point is that this could have happened to any small business in terms of the attack and fallout. Compounding the problem is that, if this theft had affected an individual, at least the FDIC would have made them whole. But small-business accounts aren't protected. So they are out the money unless they have the means to sue and the amount of loss is more than the cost of litigation.

Also, this is the silent crime. Small businesses that have been hit do not have PR shops or press agents and have little reason to let the public know they have been impacted. And the banks have little incentive to tell consumers that their fraud detection and passcode methods do not actually work against such threats. So while this cybercrime is widespread, you do not hear about it and that leaves more and more companies unaware that they need to do more.

SMBs at Risk

Unfortunately, this example shows just how vulnerable small- and mid-sized businesses can be and demonstrates the potential fallout of not having a strong cyber defense. There is no clear law or legislation that protects companies or provides guidelines on what they, their vendors or their financial institution need to have in place to protect sensitive data.

It also varies from state to state, so the burden is on each company to figure it out relative to their situation and possible exposure. It often comes as a surprise to companies I speak with; small- and mid-size businesses do not have the same protections as individuals. Again, it falls on their shoulders to ensure they are protected.

And just because you are a small business doesn't mean cybercriminals aren't going to target you. In fact, according to the Federal Communications Commission, three of every four small- and mid-sized businesses report being affected by cyberattacks.

An employee may get an email that looks valid and opens it, clicking on a link. It turns out to be a phishing scheme. It's happened time and time again with an array of targets including huge companies like Google, University of Wisconsin-Milwaukee, a Dallas-based business telephone equipment company, a Missouri dental practice and even cities such as Brigantine, New Jersey.

Security 101

The good news? There are inexpensive and intuitive tools to combat this kind of threat. So what are small and large enterprises, financial institutions and governments to do?

First, in my mind, are the cybersecurity basics — or table stakes, as you might call them — for online security. Employees must have at least basic training on security practices to protect sensitive business information, communication and transactions.

Organizations also need to ensure that computers and networks are protected from viruses, spyware and other malicious code. A firewall must be in place — not only at the point of connection to the Internet but on all computers, including laptops used to conduct company business. And, finally, the proper settings must be routinely checked for vulnerabilities and attacks.

Education, coupled with dedicated perimeter security solutions, provide the first basic layer of protection for businesses and its employees.

Another key to cybersecurity across an organization pertains to the downloading of software. I cite Brian Kreb's blog from May 2011 — "Krebs's 3 Basic Rules for Online Safety" — where he gave three basic rules for online safety in this area.

- First, **"If you didn't go looking for it, don't install it."** You are taking a great risk by downloading software that you don't directly know.

- Second, **"If you installed it, update it."** Basically, keep up with new versions of software because they include updated security for vulnerabilities that have been found in earlier versions.

- And finally, **"If you no longer need it, remove it."** Unneeded software can slow down your machine and eventually open it to a wider array of breaches. In the end, it is all about keeping networks, computers and devices protected to help thwart the opportunity for someone to breach your infrastructure.

Identity-Based Security

Finally, to truly secure your environment, you need a layered, identity-based security solution. You cannot have security and trust without knowing who or what is on both ends of a transaction.

To have that trust you must understand how digital identities are changing. Today's identities go well beyond people and how we have traditionally thought of identity. Digital identities now include kiosks, servers, routers, mobile devices, applications, ATMs and even power meters. This next generation of digital identities, including devices and application objects, will dwarf human identities in the next five years. Identity-based security brings this all together with the right level of security, enablement, risk and compliance to any transaction — regardless of identity type.

So, what do you need to know to secure identities?

You need to control physical and logical access to your facilities, computers, networks and any other devices that house important information or have access to your networks. And, increasingly, you will need to manage the "mobile" access of smartphones and tablets. Mobility has come of age and is the next wave of innovation — for good and for bad.

Of particular interest to this Subcommittee due to its jurisdiction, security may also rely on utilizing various telecommunications networks to conduct a single transaction. Verifying an online transaction by stepping outside that band is one simple example. Specifically, one option for parties conducting a transaction that is occurring over wired Internet connect is to agree to speak over a different network, perhaps by using a cell phone, to confirm the

transaction and the identity of the users. That would ensure that any connection that may have been compromised is quickly identified before a transaction is completed.

Lastly, you need to ask your financial institution how your business is protected should it become a victim of a cyber fraud. You may be surprised that current regulations leave many small businesses unprotected, as we saw with the case of Hilary Machinery. The ball is in your court.

You cannot assume business accounts are covered under the same federal protection as consumer accounts. Any business needs to ask its bank what current security measures it has in place. For the reasons I outlined earlier, the threats are constantly changing and, therefore, accounts must be protected against the latest threats. Financial institutions must invest in security platforms that provide the flexibility to implement new approaches and adapt to future challenges.

What I have outlined is a layered security approach, which is necessary to ensure that the right level of security is being applied to the access or transaction that is being requested. Identity-based security solutions, like those from Entrust, help you do just that.

Action Items

With all of this in mind, and recognizing that this is not a legislative hearing on specific remedies, there are still three key points that Washington should keep in mind.

First, cyber security legislation must ensure there is proper corporate governance within an organization to ensure someone with appropriate authority is responsible for overseeing the cybersecurity program. It must require and recognize that cybersecurity is not a one-time fix, as was Y2K, but requires continued vigilance since threats continue to evolve rapidly.

Second, the Federal government needs to work more closely with the private sector to exchange critical information about the threats that each experiences. A perfect example of the problems that face the government and protecting itself came to light via the hacking of a well-known security company that resulted in the compromise of three Department of Defense contractors and potentially critical DOD intelligence. All three attacks leveraged the security information gained in the hack of the cybersecurity product company.

This kind of situation is persistent and we have been asking the appropriate agencies to work with us to deter further damaging breaches. Congress needs to direct the government's intelligence community to work more closely with cybersecurity companies and to share vital information on evolving threats, attack methods and how to defend against threats.

Third, the private sector would also benefit from an education or awareness campaign. While large enterprises have information security personnel, many small and medium businesses do not. The same cybersecurity companies mentioned above could work with the Department of

Commerce and the Small Business Administration to make this information available to these smaller enterprises via webinars, online guidance and checklists. The weakest link in a chain remains a real threat in the cyber world and helping educate smaller entities is a vitally important part of the puzzle.

Thank you again for this opportunity to testify and look forward to any questions you may have.

Mr. WALDEN. Mr. Connor, thank you. Excellent testimony. I think we are going to have to recess so we can all go deal with our own campaign accounts, and we will be back in about an hour. We really appreciate it, and we look forward to getting into questions with you and exploring it further.

We are now going to go to Mr. Robert Dix, who is Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks, which I believe is from your district.

Mr. DIX. Proudly.

Mr. WALDEN. We are delighted to have you here. Thanks for coming the distance to share your wisdom with us, and please proceed.

STATEMENT OF ROBERT B. DIX

Mr. DIX. Thank you, Chairman Walden, Ranking Member Eshoo and members of the subcommittee. Good morning. Thank you very much for inviting me to testify about cybersecurity.

Juniper Networks is a publicly held private corporation, hardware and software manufacturer, headquartered in Sunnyvale, California, with offices and operations around the world. Information technology and communications networks are embedded in all manner of the Nation's critical infrastructure including power plants and the electrical grid, water filtration systems, financial systems and transportation networks, just to name a few.

While sectorwide risk assessments conducted or being conducted in the IT and communications sectors validate that networks are resilient, it is important to acknowledge that the risk continues to grow and change and our efforts to protect and prevent must be sustained and agile. In recognition of this reality, the private sector is working every day to protect against cyber threats through self-driven research and innovation, industry collaboration, and partnerships with government.

Let me share just a few examples. In 2007, a group of private sector companies came together to address the issue of software assurance and improving the development process integrity of software and hardware products. SAFECode, the Software Assurance Forum for Excellence in Code, is a group of companies and subject-matter experts that has set aside their competitive interest to gather and share industry best practices through a series of written deliverables that are available not just to the participating companies but to the industry at large.

Additionally, in 2008, a group of private sector companies came together to address the need for collaborative, global incident response by forming ICASI, the Internet Consortium for Advancement of Security on the Internet. Once again, the participating companies who compete vigorously in the marketplace routinely share information in an effort to mitigate anomalous and abnormal network activity globally because the cause is greater than any one company.

Across the 18 critical infrastructure sectors, we have organizations such as ISACs, Information Sharing and Analysis Centers, since 1988 working on the operational issues. Additionally, we have sector coordinating councils that were derived as a result of the National Infrastructure Protection Plan in 2006.

The Partnership for Critical Infrastructure Security is the cross-sector coordinating council representing all 18 critical infrastructure sectors and working with the Federal Senior Leadership Council under the NIPP partnership framework to advance the mission of critical infrastructure protection and cybersecurity. In fact, we are currently working with the administration on the implementation around Presidential Policy Directive #8 for national preparedness and the review and update of HSPD–7 regarding an all-hazards approach to critical infrastructure protection and cybersecurity.

Mr. Chairman, the number of users connecting to the Internet and other networks will continue to grow. Global Internet traffic is increasing at a rate of 40 to 50 percent a year and is expected to grow to 4 billion users in 2013. The explosion in the use of smartphones and tablets and the advent and growth in the use of social media is rapidly changing the workplace and how we communicate—example, an average of 10,000 tweets per second the last 3 minutes on the Super Bowl on Sunday evening—while introducing cyber risks in a way that few of us could have imagined only a short time ago. This is the essence of technology. It enables us to do what we never could have imagined, and that includes those with nefarious motives. The convenience of the technology has changed banking, purchasing, and sharing of personal financial information.

So it is only reasonable to expect that the conversation about cybersecurity must include a discussion about economics but there are two sides to this coin. If we focus only on technology and technology development, we are likely to miss the opportunity to examine the challenges and impediments to technology and solution adoption. The market is delivering innovation at an unprecedented pace in history. However, the evidence would suggest that adoption of available solutions has not kept pace and should be a topic of further examination and discussion. Many low-cost and no-cost solutions are available to improve any users' protection profile. Accordingly, there are many things we can do together. It is reported by reliable sources that some 80 percent of the exploited vulnerabilities are the result of poor or no cyber hygiene. For me, this is basic blocking and tackling. If we can raise the bar of protection, it makes it more difficult and more costly for the bad guys to do harm.

When our Nation was confronted a couple of years ago with the threat of the H1N1 virus, we mobilized as a Nation to warn and advise folks how to protect themselves from the risks of infection. We have the opportunity to use that same model for a sustained awareness program to help educate citizens, small business, students, nonprofits, and other stakeholders how to protect themselves from the risks of malware, phishing, and other forms of infection in cyberspace.

Chairman Walden, Ranking Member Eshoo and members of the subcommittee, we must move beyond just thinking about the challenges of today to thinking about the risk profile of tomorrow. Today's cyber attacks are more complex and often difficult to detect and can target classes of users, even specific users, gaining access to valuable data and causing significant harm. With a commitment

to working together in a collaborative manner, the United States will lead the effort to the protection, preparedness, and resilience of critical infrastructure and cybersecurity.

On behalf of my colleagues across the industry and the proud employees of Juniper Networks, I thank you again for the opportunity to testify before you this morning. The threat is real, the vulnerabilities are extensive, and the time for action is now. The American people are counting on us to get this right and the private sector looks forward to continuing the collaborative relationship between Congress, the administration, and private industry on this important issue. Thank you.

[The prepared statement of Mr. Dix follows:]

"Cybersecurity: Threats to Communications Networks and Private Sector Responses"

Statement of Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection
Juniper Networks

Hearing before the

U.S. House Committee on Energy and Commerce
Subcommittee on Communications and Technology

February 8, 2012

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, good morning. Thank you for inviting me to testify about cybersecurity threats to communications networks and private sector responses to those threats.

My name is Bob Dix and I serve as Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks. Juniper Networks is a publicly-held private corporation headquartered in Sunnyvale, California, with offices and operations around the world. We deliver trusted, high-performance networking and security solutions that help public sector agencies, private enterprises, and service providers deploy networks that are open, scalable, simple, secure, and automated. Juniper's portfolio includes software, silicon, and systems for routing, switching, and security. U.S. Government customers (spanning civilian, military, and intelligence functions) rely on Juniper solutions for secure remote access, Network Access Control solutions for large agency enterprises, secure virtualization solutions for consolidated data centers and cloud computing, as well as mobility solutions.

Nature of Cybersecurity Threats

Despite its prevalence in our work, personal and everyday lives, at times we need to be reminded that the Internet was not engineered or built with security in mind. In fact, it has been only in recent years that security even has been included in the discussion along with performance, function, and reliability. Over time, the threats in cyber space have continued to evolve, and as we sit here today, the range of adversaries continues to expand. They continue to enhance their capabilities and their sophistication.

From script kiddies and hackers, to criminals and dissidents, to espionage and state-sponsored actors, the range of threat vectors is extensive. And let's not forget about the rogue insider. The threats have evolved from viruses, worms, and trojans, to botnets, malware, and advanced persistent threats (APTs) that are pervasive. In fact, the ongoing theft of intellectual property may present one of the most serious threats to national and economic security.

Impact of Threats on Communications Networks

Information technology and communications networks are embedded in all manner of the nation's critical infrastructure, including power plants and the electrical grid, water filtration systems, financial systems, and transportation networks just to name a few.

While sector-wide risk assessments conducted or being conducted in the IT and communications sectors validate that networks are resilient, it is important to acknowledge that the risk continues to grow and change, and our efforts to protect and prevent must be sustained and agile.

In today's increasingly connected world, the move to cloud computing and the explosion in the use and proliferation of mobile devices and applications mean that we must be able to rely on the resilience of the network more than ever.

An intrusion into the network with a malicious payload can produce a significant disruptive impact with potentially serious functional, economic, and security ramifications.

Private Sector Response

In recognition of this reality, the private sector is working every day to protect against cyber threats through self-driven research and innovation, industry collaboration, and partnerships with government.

Information technology and communications companies invest significant budget and resources to drive the innovation and deliver solutions that will improve the protection, preparedness, and resilience of our public sector and private industry customers from the impact of cyber attacks.

As an example, Juniper Networks invests heavily in research and development into next generation networking and security solutions. In calendar year 2011 alone, Juniper spent more than $1 billion on research and development.

This is but one example of the R&D investment made by a tech company. It is this type of investment that is driving much of the innovation that will change the world in terms of the way we communicate and operate in cyberspace. Collectively, we should be encouraging and enabling such investment and job creation.

In response to the growing cybersecurity challenge, the private sector has initiated myriad activities to address many dimensions of the various issues. Additionally, many companies and organizations in the private sector have committed resources, knowledge, expertise, and insight in working with our government colleagues through a range of public-private partnerships. Let me share just a few examples.

In 2007, a group of private sector companies came together to address the issue of software assurance and improving the development process and integrity of software and hardware products. SAFECode (Software Assurance Forum for Excellence in Code) is a group of companies and subject matter experts that have set aside their competitive interests to gather and share industry best practices through a series of written deliverables that are available not just to the participating companies, but to the industry at large. SAFECode has worked closely with the DHS Software Assurance Forum and others.

Additionally, in 2008, a group of private sector companies came together to address the need for collaborative, global incident response by forming ICASI (The Internet Consortium for Advancement of Security on the Internet). Once again, the participating companies, who compete vigorously in the marketplace, routinely share information in an effort to mitigate anomalous and abnormal network activity globally. Because the cause is greater than any one company.

Resulting from PPD-63 in 1998, which specifically addressed critical infrastructure protection and cybersecurity, and responding to a call for a public-private approach, the private sector formed Information Sharing and Analysis Centers (ISACs) across the private sector critical infrastructure community to enhance operational capabilities within and across sectors and their member companies.

At the request of the government, and concurrent with the development of the National Infrastructure Protection Plan (NIPP) in 2006, Sector Coordinating Councils (SCCs) were formed in the then 17 and now 18 critical infrastructure sectors to address policy and strategy issues

around risk assessment and risk management efforts to improve the protection, preparedness and resilience of our nation's critical infrastructure. These councils are self-organized and include participation across a broad range of companies, organizations and associations. They work closely in most sectors with their ISAC counterparts to include the operational component of the collaboration.

The Partnership for Critical Infrastructure Security (PCIS) is the coordinating body for the private sector critical infrastructure sectors and works closely with the Federal Senior Leadership Council under the NIPP Partnership Framework to advance the mission of critical infrastructure protection and cyber security. I should note that I serve as chairman for the PCIS. The partnership framework includes state and local government. Currently, the PCIS is working with the Administration on the implementation of PPD – 8 around National Preparedness; and the review and update of HSPD – 7 regarding an all hazards approach to critical infrastructure protection and cyber security.

Given that we cannot be truly successful unless we continue to advance the opportunities for collaboration between industry and government, and acknowledging that this is truly a shared responsibility, it is necessary to leverage all such opportunities. Through advisory committees such as the President's National Security & Telecommunications Advisory Committee and National Infrastructure Advisory Council, some of the great minds and technical experts in the world in government and the private sector come together to tackle hard challenges.

It is also important that we periodically test our preparedness and resilience through planned exercises. Over the past several years, industry and government have worked together to

design, plan, and execute the Cyber Storm series of Tier II national cyber exercises. This year, National Level Exercise 2012 will focus on cyber as a Tier I national exercise and presents an opportunity to test improvement actions implemented as a result of lessons learned from previous Cyber Storm exercises, as well as testing our national preparedness and resilience, including the current elements of the National Cyber Incident Response Plan and the National Cyber Risk Alert Level.

The information technology and communications sectors continue to innovate, making networks smarter and more resilient, looking to build more intelligence into the networks to protect the confidentiality, integrity, and availability of the data and to improve access and authentication controls to provide trust and security for online transactions and interactions.

Just a few weeks ago, a group of major Internet companies announced a voluntary initiative to prevent spam and phishing e-mails. PayPal, Yahoo, Microsoft, and Google are working on a new system to authenticate e-mail senders that will make it more difficult for bad actors to conduct their attacks through fraudulent e-mails.

These are just a few of the examples of productive efforts by the private sector to drive solutions, as well as evidence of the success that we can achieve when we work together in a truly collaborative manner.

Going Forward

Mr. Chairman, the number of users connecting to the Internet and other networks will continue to grow. Global Internet traffic is increasing at a rate of 40-50 percent per year. There are now

almost two billion Internet users and that number is expected to grow to four billion by 2013. It is also important to remember that the risk in cyberspace is dynamic. Threats and vulnerabilities evolve rapidly and the capability to manage and mitigate risk depends on an ability to be and remain agile and able to react quickly.

The technology and types of devices will continue to evolve and applications will continue to be delivered into the marketplace at a frenetic pace. The volume of data and video is growing exponentially and the demand for capacity, scale, and security will be paramount. The world of computing, storage, and networking is rapidly changing and evolving to meet those demands and security must be imbedded in the technology, the strategy, and the policy going forward.

The explosion in the use of smart phones and tablets and the advent and growth in the use of social media is rapidly changing the workplace and how we communicate, while introducing cyber risks in ways that few of us could have imagined only a brief time ago.

This is the *essence* of technology. It enables us to do to what we never imagined – and that includes those of us with nefarious motives. The convenience of technology has changed banking, purchasing and the sharing of personal financial information.

It is imperative that all of us acknowledge that cybersecurity is truly a shared responsibility, and that managing risk will require a true collaborative approach between government and the private sector. The private sector owns and drives the majority of the innovation, and also owns and operates the majority of our nation's critical infrastructure. The private sector also has access to important information that is relevant to the government, while the government has

access to much threat intelligence information that would be valuable to the private sector in advancing risk management activities to protect the network and the data.

We have the opportunity to seize this moment in time to build on the Comprehensive National Cybersecurity Initiative; the Cyberspace Policy Review; the National Strategy for Trusted Identities in Cyberspace; and many other efforts to improve the national and economic security of our nation.

The conversation about cybersecurity must include a discussion about the economics. But there are two sides to this coin. If we focus only on technology and technology development, we are likely to miss the opportunity to examine the challenges and impediments to technology and solution *adoption*. The market is delivering innovation at an unprecedented pace in history. However, the evidence would suggest that adoption of available solutions has not kept pace and should be a topic of further examination and discussion. Perhaps the business case or value proposition for investment has not been adequately communicated to user constituencies of all levels, from home users, to small business, to academic and non-profit institutions and even to large enterprises.

Many low cost and no cost solutions are available to improve any user's protection profile. Incentives for businesses such as liability protection, market recognition and differentiation, and even tax incentives may spur investment in an advanced cycle.

Accordingly, there are many things that we can do together. It is reported by reliable sources that some 80 percent of exploitable vulnerabilities are the result of poor or no basic cyber

hygiene.[1] For me, this is basic blocking and tackling. If we can raise that bar of protection, it makes it more difficult and more costly for the bad guys do harm.

When our nation was confronted a couple of years ago with the threat of the H1N1 virus, we mobilized as a nation to warn and advise folks how to protect themselves from the risk of infection. We all remember the messages, public service announcements, posters, radio, TV, and Internet messages regarding the need to cough into our sleeves, wash our hands, and other protective measures to secure our health. The effort included the CDC, HHS, and other federal departments and agencies, along with many non-profits, businesses, and organizations.

We have the opportunity to use the same model for a sustained awareness program to help educate citizens, small businesses, students, non-profits and other stakeholders on how to protect themselves from the risk of malware, phishing and other forms of infection in cyberspace.

Many federal departments and agencies interact with citizens and businesses routinely. Leveraging the Small Business Administration; the Internal Revenue Service; the U.S. Postal Service; the U.S. Department of Education; and others would provide an ability to scale the messaging across a wide range of the population. Perhaps we could even convince every Member of Congress to include a link on their constituent website that directs folks to where they can get more information about protecting their health in cyberspace.

---

[1] *See* CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE, HEARING BEFORE THE U.S. SENATE COMM. ON THE JUDICIARY SUBCOMM. ON TERRORISM AND HOMELAND SECURITY 111th Cong., 2d Sess. 19 (Nov. 17, 2009) (statement of Mr. Richard C. Schaeffer, Jr., Director, Information Assurance Directorate, National Security Agency).

We should be proactively enlisting the expertise and innovation of telecommunications service providers and content providers to engage in the path forward. Many are already engaging in innovative efforts to identify and notify consumers about infections.

Many of you on the Subcommittee and Full Committee have been actively involved in attempting to address the issue of facilitating the exchange of intelligence information and creating a true partnership between government and industry to build enhanced situational awareness to improve detection, prevention, and mitigation of cyber events that may become incidents of national consequence.

Though the private sector is doing work internally to address the threat, the government has an important opportunity to do a better job of providing threat indicators and intelligence to private industry. Far too often, government continues to compartmentalize and restrict access to relevant information. In order for private industry to be able to prevent and mitigate threats, industry must have access to the threat information that the government possesses. Keep in mind, this does not mean industry needs access to sources and methods – rather, access to information about Tactics, Techniques, and Procedures will improve the ability to manage risk, acknowledging that we simply cannot protect everything all the time...just as is true in the physical world.

With this in mind, legislation introduced by a Member of this Subcommittee, Rep. Mike Rogers (R-MI), in his capacity as Chair of the Permanent Select Committee on Intelligence, H.R. 3523, the "Cyber Intelligence Sharing and Protection Act of 2011," would amend the National Security Act to facilitate the sharing of cyber threat intelligence with eligible private sector entities.

Wisely, the bill protects the sensitive nature of such information by requiring that security clearances be granted as necessary to the relevant private sector entities. In addition, the bill ensures that that the private sector treats the sensitive information as such – private sector recipients of the threat information may use it only to protect rights and property. Finally, the bill confers liability protection for companies that choose to protect their networks or share information based on the authorities provided under the bill.

This legislation will add an arrow to the protection quiver by addressing a key impediment to building cyber situational awareness.

Through the development of the National Cyber Incident Response Plan, and many other examples, we have proven time after time that when we work together, the results are more productive.

Accordingly, going forward we need to work together to map the gaps in technology as well as legal and policy impediments to improving our cyber security posture. Building on the current efforts to conduct risk assessments and risk management plans in each sector through the Sector Coordinating Councils, we can work to refine high probability, high impact risk; the recommended protective measures; and potential gaps that would be candidates for research and development activities, either in the private sector or government. Working together, we can continue to collaborate with the National Institute of Standards and Technology (NIST) and other standards bodies to develop and update recommended security provisions to enhance overall risk management.

Conclusion

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, we must move beyond just thinking about the challenges of today...to thinking about the risk profile of tomorrow. Today's cyber attacks are more complex and often difficult to detect, and can target classes of users – even specific users – gaining access to valuable data and causing significant harm.

We have an opportunity to operationalize information sharing, analysis, and collaboration to build true situational awareness and an enhanced common operating view of the cyber domain to improve detection, prevention, and mitigation.

We need to continue to examine opportunities for developing a cyber savvy workforce and overall population.

With a commitment to working together in a collaborative manner, the United States will lead the effort to improve the protection, preparedness, and resilience of critical infrastructure and cyber security.

On behalf of my colleagues in the industry and the more than 9,000 proud employees of Juniper, I thank you again for this opportunity to testify on cybersecurity as it relates to communications networks. The threat is real...the vulnerabilities are extensive...and the time for action is now. The American people are counting on us to get this right. And the private sector looks forward to continuing the collaborative relationship between Congress, the Administration, and private industry on this important issue.

Mr. WALDEN. Mr. Dix, thank you very much for sharing those comments with us.

We now go to Dr. James A. Lewis, Director and Senior Fellow, Technology and Public Policy Programs, Center for Strategic and International Studies. Dr. Lewis, thank you for being with us. We look forward to your testimony as well.

STATEMENT OF JAMES A. LEWIS

Mr. LEWIS. Thank you, Mr. Chairman, and I would like to thank the committee for this opportunity to testify.

One thing that military and intelligence experts would agree on is that the cybersecurity problem is getting worse, not better. There is straightforward evidence that what we are doing now isn't working. Most of these experts also believe that we will not change our laws and policies until there is a crisis. I hope they are wrong.

We all recognize the growing dependence of our economy on cyberspace and the risk this creates. Director of National Intelligence Clapper testified last week about how Iran, which is eagerly developing cyber attack capabilities, is losing its reluctance to attack the American homeland. FBI Director Mueller testified, as you heard, that the threat we face now comes from terrorism but in a few years the bigger threat will come from cyber attack.

The ability to launch damaging attacks is spreading from a few advanced nations to many countries and many hostile groups. There is disagreement among when hackers will disrupt critical services in the United States, but most estimates put it at sometime in the next couple of years. Cyber crime and espionage are rampant now, costing American jobs and damaging American economic competitiveness and national security.

This morning, I was trying to think of what I could say that would be a little different, and I remembered that I attended, as a back bencher for the Director of Central Intelligence, some of the first meetings in the Clinton administration on commercializing the Internet. Back then, we thought that it would be used for e-commerce, that it would be eBay and Amazon. We didn't expect a global network that would become the premier vehicle for espionage and a potential avenue for attack. We thought that if we made tools and information available, if we freed up encryption, companies and people would voluntarily secure the networks. I am a little embarrassed sometimes when I see a paper I wrote for the White House in 1996 that said that because I was wrong. We made the same mistakes in our approach to critical infrastructure protection.

There were three big errors. The incentives for cybersecurity vary from company to company and sector to sector, and usually they are insufficient. There are legal obstacles that limit the ability of governments and companies to cooperate and to share information. And in any case, we need a coordinated defense, not a grab bag of individual actions. Finally, we did not expect to face world-class opponents, as you heard from some of the earlier testimony, even midrange opponents with access to world-class tools. We overestimated incentives and underestimated threats and legal obstacles, and I would like to point out that Congressman Rogers' bill would be very useful if we could get it passed in removing some of the legal obstacles that hamper our ability to provide an ade-

quate cyber defense. A serious defense requires coordination and mandatory action. The big telecom companies are pretty good at securing themselves and don't need more regulation but the other sectors are in bad shape. Some people say regulation is burdensome, but if we do not hold critical infrastructure to mandatory standards, we guarantee a successful attack. Nor does regulation damage innovation. An unregulated Internet is not a substitute for a business-friendly environment that innovation really needs.

Partnership and cooperation must become more than an exchange of slogans. Australia has a good model, we heard about that, where the government encouraged Internet service providers to develop a code of conduct to deal with malware. That appears to be working. We are considering in the United States similar options.

Finding ways to expand the use of DNSSEC. DNSSEC is a good story. This is a fundamental rule set, the addressing framework for the Internet. We identified problems with it 20 years ago. We identified fixes for it 12 years ago. We have not implemented these fixes. This is one where finding some new approach to get people to move faster would be really crucial. The Defense Industrial-Based Initiative, which shares classified threat information, is another good example of how to do real cooperation.

There are many opportunities to improve cybersecurity, but taking advantage of them will require a new approach. I think one thing I can say is everyone wants to make things better. We all realize the scope of the problem, and everyone wants to do stuff. Hearings like this provide an opportunity to find that new approach that will truly serve national security.

I thank the committee for the opportunity and look forward to your questions.

[The prepared statement of Mr. Lewis follows:]

Testimony
Cybersecurity, Threats to Communications Networks, and Private-sector Responses.
House Committee on Energy and Commerce
Subcommittee on Communications and Technology
James A. Lewis, Center for Strategic and International Studies
February 8, 2012

Internet technologies are so desirable and so efficient that people proceed to use them without regard to risk. This means we are building vulnerability into the fabric of our economy. A disregard for risk has always been part of the adoption of new technologies, but past technology, risks were localized and not systemic: the internet is different. The behavior is the same, but the global scope, the incredible rapidity of connection, and inadequate technology changes the nature of risk and increases it.

Our vulnerability as a nation is increasing as our dependence on digital network technologies grows and as the skill and number of our opponents increases. Our cyber defenses have not kept up. This is largely a political problem. Our policies and our laws are inadequate. We now know how to reduce risk on networks, but we have chosen not to do so. From a planning perspective, it is best to start by assuming that no commercial or unclassified network is secure.

It would be easier to solve this problem if there was some big dramatic event – the Pearl Harbor everyone talks about – or if our opponents were foolish enough to start a cyber car. Neither of these is likely, however. There are of course countries with the ability to launch very damaging attacks – of the five or six countries with advanced cyber capabilities, two – Russia and China – bear us ill will and would use cyber attack in any conflict with the United States. But barring some miscalculation, they will avoid any action that could trigger an American response. They will stay below the threshold of the use of force that would justify an American military response. If they were to attack, however, we are defenseless because of our inability to move beyond antiquated notions of security.

The problem of lacking an adequate defense involves more that military conflict with Russia or China. Many other nations are acquiring cyber attack capabilities. The two most dangerous are Iran and North Korea. Anti-government groups, criminals and perhaps jihadis are also acquiring these capabilities. Two likely scenarios are worth considering, involving Iran and anarchic groups who may use the label "Anonymous."

Iran has been building its cyber attack capabilities for years. It is difficult from open source material to get a good picture of Iranian capabilities. The task is also complicated by ridiculous claims that come from Iran, such as the claim that Iran hacked into a U.S. drones. This is a nation, after all, that will routinely use "photo-shop" to make its missiles or other weapons look better. But just as Iran has doggedly pursued nuclear weapons, it has doggedly pursued cyber attack capabilities. Iran routinely probes Israel's networks to test its cyber capabilities. Iran was probably responsible for hacking the Dutch company "Digi-Notar" to acquire certificates that let them intercept communications for Iranian dissidents. Iran has close defense relations with China and Russia and may receive assistance in developing cyber capabilities. And Iran may feel that it is justified in launching a cyber attack since it was the victim of Stuxnet, the most

sophisticated cyber attack seen to date and which Iran blames on Israel and the U.S.

Director of National Intelligence James Clapper testified last week that Iran is losing its reluctance to strike domestic targets in eh U.S. It is easy to imagine the Iranian miscalculating, overestimating their ability to conceal their tracks, and launching a cyber attack. Perhaps they will use a proxy like Hezbollah or Hamas in an effort to conceal their involvement and to further complicate any American response.

Another likely source of attack in the future comes from the group "Anonymous." Calling "Anonymous" a group is something of a misnomer. Anyone can claim to be part of Anonymous. It can include teenagers with a grudge, the kind of anarchists who wear black masks and smash shop windows in violent protests, cyber criminals and perhaps even foreign intelligence agencies using the label as a convenient disguise. Anyone can engage in a malicious act and claim it "Anonymous."

This means it is very difficult to assess the range of cyber attack capabilities those who claim to be Anonymous may possess. Most of the actions attributed to Anonymous have been basic and Anonymous tends to exaggerate. But some in the hacker community say that some of the most skilled hackers in the world are among the ranks of Anonymous. We do have some idea of their motivations, which are anti-government and anti-American, and of their inventiveness, as they have been able to exploit corporate networks with ease.

If Iran or anarchists groups launched a cyber attack, what would it look like? It would likely not be catastrophic. Cyber "weapons" cannot cause mass casualties or mass destruction. Our own Department of Defense regards cyber as a "support weapon." A cyber attack will not be militarily decisive, but it will provide real advantage in any military conflict. Three recent incidents give us an idea of what a real cyber attack would look like.

Computer error caused the flash crash of 2010, when the stock prices temporarily collapsed. In this case it was inadvertent, but a moderately skilled attacker could be able to duplicate the effect. A more damaging attack might involve disruption and erasure of financial data. This kind of disruption of "Wall Street" would be attractive to some groups. Even selective targeting of a specific company or bank and its customers would cause an uproar. The 2003 Northeast blackout was also caused by inadvertent computer error. A moderately skilled attacker would also be able to duplicate this. It is possible to launch cyber attacks that are more damaging and which cause actual physical destruction, but these capabilities appear to be beyond what Iran or Anonymous could acquire in the near future.

Similarly, it is possible to interfere with other utilities. Anarchist might enjoy simultaneously turning all the traffic lights in the city green or having them change randomly. They could interfere with the water supply. Public utilities, financial services, communications – what we have come to call "critical infrastructure," are natural targets. They are routinely targeted by military planning and guerrilla operations. Before, insurgents might have pulled down power lines or blown up a substation. Soon, they will be able to use computers.

Of these, the electrical power supply is the most likely target. The cost-benefit ratio of attacking

this sector favors our opponents. Interrupting the flow of electrical power would be very disruptive, since we depend on electrical power, and it is the easiest to attack. Repeated studies have shown that control systems and critical networks are vulnerable and that companies may not even be aware of their vulnerability. In the future, when hackers want to protest bills like SOPA, they may turn off the lights in Washington instead of voluntarily blacking out a few websites.

The third predictive incident was the December 2008 penetration of DOD's classified network SIPRNET. This was carried out by a foreign intelligence service. No data was exfiltrated but the U.S. was unable, for a period of days, to remove the malware from SIPRNET. In a war, the foreign opponent could have used this malware to erase or scramble vital military data, disruption our command and control and greatly hampering U.S. operations. Of course, our most advanced opponents could also cripple critical infrastructure, but the first and perhaps only cyber attacks will be against military networks.

Incidents like SIPRNET or Stuxnet show that advanced attackers can penetrate any network. The crisis created by SIPRNET led DOD to take a number of steps to improve its defenses, including the creation of Cyber Command, imposing new requirements on defense contractors (whose networks are routinely targeted) and finding ways to share information with contractors and internet service provider. DOD recognized the scope of the problem and took steps to reduce risk. The same is true at other U.S. agencies that were the victim of cyber espionage. Others have not. There is little incentive to spend money to improve defenses

Other scenarios are of course possible. None of these incidents were catastrophic, and despite the weekly barrage of stories about cyber attacks and cyber war, most malicious activity in cyberspace involves either espionage or financial crime. Criminal acts are pretty straightforward – weak cybersecurity allows criminals to extract money. The best estimates suggest that this financial crime probably costs the U.S. several hundred million dollars a year. Most advanced cyber criminals live outside the U.S. or Western Europe, in countries that act as sanctuaries for cybercrime. Their activities are largely risk free, in that the chances of arrest or imprisonment are minuscule. They do this because cyber criminals form "proxy forces," irregulars whom the Government can call upon to carry out hostile cyber actions – this is what we saw in the politically coercive cyber activities aimed against Estonia and Georgia. Unwillingness to abandon these proxy forces explains much of the lack of progress in international cooperation against cybercrime.

There is a thriving black market in cybercrime tools and techniques and one issue to watch is how long it will take for advanced attack capabilities to appear for sale in these in these markets. Since there are links between governments with the most advanced cyber-attack capabilities and criminal proxies, we can expect that advanced capabilities will flow into private hands.

Espionage is directed against both government agencies and private companies. It is carried out by both intelligence agencies and private actors. American companies are prime targets. There is little public data on the full extent of their losses, since companies conceal when they have been hacked. But the U.S. has seen sensitive military technologies extracted by foreign opponents. Economic espionage against American companies is rampant, a symptom of the poor

network security prevalent in the U.S. and the lack of agreed international norms and penalties for malicious cyber activities.

Measuring the effect of economic espionage is difficult. Some cases are easy. When a foreign competitor steals confidential business information, such as oil exploration data or contract negotiations data, they get an immediate advantage that could be worth, in some instances, hundreds of millions of dollars. When they steal designs for advanced technology, as was the case in December 2010 when seventy U.S. high tech companies were hacked and lost data, it may take the opponents several to translate this data into actual products. But the long-term effect is to damage America's trade competitiveness and technological leaders, and to cost American jobs.

Fixing the problem of weak cybersecurity will not be easy. It will require a wide-ranging approach that works on an international, national, and individual level. The first element is greatly expanded international agreement between governments on their responsibilities in cyberspace. This will need to include common understandings on how international laws apply, including the laws of armed conflict, expanded law enforcement cooperation, better internet governance, and a stronger enforcement of trade rules, including penalties for failing to protect intellectual property.

Part of this will require developing and publicizing military doctrine and policies to warn potential attackers. A more difficult issue will require deciding what role the military and intelligence agencies will play in defending domestic networks. This is unavoidable because agencies like NSA are the most skilled and have the most knowledge about cyber defense, but our laws limit their involvement in domestic activities.

A strong national defense will involve improving cybersecurity in selected critical infrastructure sectors – power and energy, finance and telecommunication. Some of these sectors already do a good job and very little additional government action is required. Telecommunications companies have a business interest in providing reliable service to their customers. The same incentives do not exist in most other critical sectors, however, and government intervention will be necessary in those cases.

The first of these additional steps is to incentivize "enterprise" level defense by critical infrastructure companies. Critical infrastructure companies must be incentivized to provide adequate digital security, particularly for securing industrial control systems that control crucial machinery. The Stuxnet attack successfully targeted these control systems, and hackers can use the internet to remotely access controls systems, disrupt key services and cause massive machines to self-destruct. Most control systems are vulnerable to cyber attack because of their age and configuration, and because they are often connected to the internet in ways that lets' them be attacked from anywhere on the globe. When you ask many critical infrastructure companies if their control systems are connected to the internet, most will tell you that they are not. If you then examine their systems, you will find connections that they do not know about. Hackers can find these connections and use them for attacks. One DHS review found that every critical infrastructure company it examined had been penetrated and that he attackers had been lurking in the computer systems for an average of eighteen months.

Companies will not provide cybersecurity adequate for national security on a voluntary basis. A company may not know of the vulnerability, it may underestimate the threats it faces, and it may have no desire to spend money on security when this does not generate a return on investment. There is no disagreement that burdensome, prescriptive regulation should be avoided, but a reliance on voluntary or widely accepted business practices – what we do today – will damage national security. The best alternative to both prescriptive regulation and inadequate voluntary practices is a pragmatic, standards-based approach that sets goals and then lets companies decide how best to achieve them.

There are now standards and practices, building on research carried out by the National Security Agency. If they are put into practice, they can significantly reduce cyber risks. .The effectiveness of these new approaches to defense can be measured using data collected from networks rather the collection of anecdotes and fables we have use in the past. We can test what works and what does not. Government can base a regulatory approach to critical infrastructure on these standards and practices. There must be decisions about which infrastructure require regulation and how regulation should be implemented, but any nation that does not put this kind of safeguards in place will ultimately be vulnerable.

The telecommunications sector is one of the truly crucial infrastructures for cybersecurity. It is the backbone of the internet and the fabric that connects us. An examination of this sector shows the complexity of the problem. The sector is already heavily regulated and it is in the business interests of major telecommunication's companies to provide reliable service. Their business models makes them the only sector with the expertise and incentives to take cybersecurity seriously, but even then there are issues and problems were uncoordinated private actin is inadequate and government intervention is needed. We may not need more regulation as much as we need insight to ensure that companies are performing at equivalent levels and to understand what threats they see.

Government needs to play a role in incentivizing and coordinating an industry wide response. An example of this kind of problem involves securing the Domain Name System – known by the term DNSSEC. DNS is the addressing system of the internet. If there was some disruption to DNS, the internet would slow to a halt or attacker would be able to hijack traffic. The problems with DNS were discovered about twenty years ago. Solutions were identified a decade ago, but the U.S. has been slow to implement them. This is beginning to change, but unevenly. Government agencies can play a coordinating and incentivizing role to promote the widespread adoption of DNSSEC, and reserve intervention only if this coordinating approach proves inadequate.

Botnets are another problem that might not require regulation. Many consumers may be unwittingly running malware and their computers may be part of a "bot." Such botnets may be used to send spam or engage in illegal activities that do not raise critical infrastructure concerns. But they may also be used to launch denial of service attacks against critical infrastructures and, in any event, create enough traffic on the network to make more egregious activity harder to detect and respond to. The ability to address infected consumer machines -- and botnets in particular -- is an important part of any critical infrastructure protection strategy.

Government agencies, the IT industry, and concerned citizen groups have engaged in a myriad of activities designed to help manage such consumer risks. They have worked to educate users about common threats and how to mitigate them, providing advice on firewalls, anti-virus, and patching. Tools have been built to automatically scan machines, patch programs, update virus signatures, and remove malware when found. As helpful as education and these tools are, they have proven to be inadequate to the task. Some consumers do not follow the guidance provided and engage in other unsafe actions. Most consumers have no desire to become IT professionals, let alone security experts, and information technology is complex enough that knowing how to protect oneself is not intuitive. As a result, many consumers may be unwittingly running malware and their computers may be part of a "bot., and computers in the U.S. are a leading source (if unwitting) of global malicious activity because of poor cybersecurity.

In this instance, the U.S. could adopt a model similar to what Australia has done to improve consumer safety. Australian ISPs have a voluntary code of conduct to protect consumers from malware and to deal with bot-nets and other consumer level problems, but this was adopted only with the strong encouragement and participation of the Government. If the companies had failed to adopt coordinated voluntary measures, there would have been regulation. The U.S. needs a similar voluntary code of conduct for ISPs, backed by government oversight, and developed using a similar voluntary and coordinated mechanism.

In thinking about cybersecurity, we still rely too much on policies created by the Clinton Administration. The 1998 Presidential Decision Directive-63 was a foundational document for cybersecurity, but the concepts and policies found in it are no longer adequate for a critical global network. PDD-63 believed that adequate cybersecurity could be achieved through voluntary measures, information sharing and public private partnerships. This may have been enough for the early days of the internet, but it is no longer sufficient.

The internet of the future will be a service. People will connect using "apps" and mobile devices whose programming will not be easily accessible to them. This will shift responsibility for security away from the "edge."
The internet will increasingly be "device-centric," further automating machines (like cars) and services without requiring constant human intervention. Commercial service providers will be at the center of the new internet, and without regulation similar to what we now use with airlines and safety of flight, public safety will be at risk.

The central problem for the U.S. will be redefining the role of government. There are clearly areas where the government should not interfere. At the same time, cybersecurity is a national security problem that requires more government involvement, not less. We often hear that the private sector owns eighty or ninety percent of the infrastructure. This idea is a leftover from the dot.com era and not very helpful. A better way to think about cybersecurity is that the private sector owns ninety percent of the targets. We do not ask airlines to protect our airspace and no one says that because the private sector owns eighty percent of beachfront property that we do not need a navy. The same logic applies to cybersecurity. You will sometimes hear that the best hackers are outside of government. Even if this is true, those hackers do not have millions of dollars in resources, access to advanced technology and other kinds of, including human spies,

and thousands of compatriots all working to undermine our defenses.

Porous technologies and weak governance make cyberspace an environment that is easily exploited by malicious actors. While we will see technological improvements over the next few decades that will reduce risk, near term improvements require changes in national policy and international cooperation. There are things we could do this year that would reduce risk, if we choose to do them. A comprehensive approach to cybersecurity can make us safer and let us take advantage of the new technologies in ways we have yet to imagine.

Mr. WALDEN. Dr. Lewis, thank you. We appreciate your testimony, and we will have a few questions for you, especially on the Australia model.

We are going to go now to Mr. Larry Clinton, President and Chief Executive Officer of Internet Security Alliance. Mr. Clinton, thank you for being here today. We look forward to your comments.

STATEMENT OF LARRY CLINTON

Mr. CLINTON. Good morning, Mr. Chairman, members of the committee.

There has been a dramatic change in the cyber threat picture in the last 18 to 24 months. Our main concern is not hackers or kids in basements. The fact that a cyber system has been breached is no longer the metric which determines whether or not an attack has been successful. Cyber attacks have grown increasingly sophisticated using what is commonly referred to now as the advanced persistent threat, or the APT. APT attackers are pros. They are highly organized, well-funded, often state-supported, expert attacks who use coordinated sets of attacking methods both technical and personal. Perhaps most indicative of these attacks is if they target a system, they will almost invariably compromise or breach it. Unfortunately, conventional information security defenses don't work against the APT. Attackers are successfully evading all antivirus intrusion and traditional best practices, remaining inside the target's network while the target believes they have been eradicated.

This doesn't mean that we have no defense. It means that we need to modernize our notion of what constitutes cyber defense. Traditional approaches including Federal regulation will not solve the problem because they are going to be largely reactive and will not stay ahead of the changing threat nature. Worse, bad regulation could be counterproductive, leading companies to expend their limited resources on building in-house efforts to meet regulatory demands rather than focusing on security.

The fundamental of stopping the advanced threat is to understand our biggest problems are not technological, they are economic. Independent research has consistently shown that the single biggest barrier to combating the cyber threat is cost. President Obama's Cyberspace Policy Review said many technical and management solutions that would greatly enhance our security already exist in the marketplace but are not being used because of cost and complexity. Just last week, Bloomberg released an extensive study that found that to reach an acceptable, not ideal, acceptable level of security in critical infrastructure would require a 91 percent increase in spending.

The private sector has been extremely responsive to combating the cyber threat. Average spending on cybersecurity in the telecommunications industry is $67 million a year with governance, by the way, including regulatory compliance, being the single biggest thought.

Despite the fact that our critical infrastructure is under constant attack, we have never had an instance of serious breakdown, mass deaths, evacuations, economic catastrophe, similar to what we have seen in the environmental area. This success is due in large part to the flexibility generated by the current system, which relies on

voluntary partnerships where an industry understands and can manage the systems best and use their intimate knowledge to respond rapidly to emerging threats in a fashion they believe can best protect the system rather than being driven by a preset government directive. Nevertheless, there is a great deal that Congress can do and the Commerce Committee can do to improve our cybersecurity right now.

First of all, we need to get the government's house in order. The National Academy of Sciences, the GAO, and just last week the DOE Inspector General have all documented systemic problems in managing government cyberspace. These need to be addressed immediately.

Second, we need to provide the right mix of incentives and regulation. For industries where the economies of the industry are tied directly to a regulatory format such as electric utilities, water, transportation, etc., the current regulatory structure can be used to motivate and fund needed cyber advancements. For industries where the economics are not inherent to a regulatory structure, adding a new regulatory structure will impede innovation and investment, making us less secure. In these sectors, we need to motivate by providing appropriate market incentives to spur greater security and investment. An excellent example of this approach is Mr. Rogers' bill, which passed the Intelligence Committee a couple of weeks ago, which uses liability reforms to stimulate additional information sharing. However, liability reform is only one of many incentives that need to be unleashed to help us secure our cyber networks. Other incentives include better use of government procurement, streamlining regulation in return for demonstrated security improvements, greater use of private insurance, and streamlined permitting and licensing. This incentive-based approach was spelled out in some detail in the ISA cybersecurity social contract in 2008 and was also endorsed by President Obama in the Cyberspace Policy Review in 2009, the multi-trade Association and Civil Liberties Coalition white paper on cybersecurity in 2010, and the House Task Force report in 2011.

A great deal of work needs to be done to fill out how these incentive models can be used in the various sectors. In the meantime, Congress ought to enact FISMA reform or to do the Rogers information sharing bill and should do a good deal to better coordinate amongst themselves. Passing that package of cybersecurity reforms would be a historic and politically achievable goal.

Ladies and gentlemen of the Commerce Committee, you are dealing with the invention of gunpowder. Mandating thicker armor is not going to work any more than building deeper moats was going to stop the horders and the invaders who invented catapults or the Maginot Line was able to stop the Germans in World War II. We need a different approach. We need a contemporary and creative approach that engages the private sector with government, not having the government control what the private sector does.

We really look forward to continuing to work with you.

[The prepared statement of Mr. Clinton follows:]

Testimony of
Larry Clinton, President & CEO
Internet Security Alliance

before the
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives

Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses."
February 8, 2012

Executive Summary (oral statement)

There has been a dramatic change in the cyber threat picture in the last 18-24 months.

Our main concerns are not "hackers" or kids in basements. The fact that a cyber system has been "breached" is no longer the metric that determines a successful cyber attack.

Cyber attackers have grown increasingly sophisticated. Not only are the tactics more complex but the number of individuals, organized groups, and nation states with these capabilities have also grown. In addition to the individual "hackers" that can do damage, we have groups of "hacktivists" that bring their political agendas from the physical world into the online world. These groups conduct denial of service attacks and trade in stolen information to push their message forward. We also see organized criminals and nation states that leverage sophisticated tools and inherent vulnerabilities in technology to gain long-term footholds on systems – this is commonly referred to now as Advanced Persistent Threat, APT.

The APT attackers are pros. They are highly organized, well-funded, expert attackers who use coordinated sets of attacking methods both technical and personal. The investment required to carry out these attacks suggests they are often nation-state supported.

Perhaps most indicative of these attacks, if they target a system they will invariably compromise, or "breach" it.

We have seen these attacks for several years in the defense sector however they have recently migrated far more broadly. The most recent research shows that responding to APT style attacks has become the major focus in industries as diverse as utilities, consumer products, financial services industrial and manufacturing sector and even entertainment and media.[1]

Unfortunately, conventional information security defenses don't work vs. APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated."

[1] PricewaterhouseCoopers. "Global State of Information Security Survey: 2012." Sept. 2011.

This doesn't mean we have no defense. It does mean we need to modernize our notion of what constitutes cyber defense. Traditional approaches, including federal regulation will not solve the problem as it will be largely reactive and not stay ahead of the changing nature of the threat. Worse, bad regulation could be counter-productive, leading companies to expend their limited resources on building in-house efforts to meet regulatory demands over actually dealing with the threat proactively.

Fundamental to stopping the advanced cyber threat is to understand that our biggest problems are not technological, but economic.

Research from Pricewaterhouse, CIO Magazine, CSIS & McAfee as well as ISA's own work has consistently shown that the single biggest problem in combating cyber threat is not technical, it is cost.

Just last week Bloomberg released an extensive study that found to reach an acceptable, not the ideal, level of security in critical infrastructure would require a 91 percent annual spending increase.

The private sector has been extremely responsive to combating the cyber threat. The private sector has been extremely responsive to combating the cyber threat. Private sector spending by US companies on cyber security has doubled in the last 5 years and is projected to be approximately 80 billion dollars for 2011[2] ---- by comparison, the official spending request for the entire Department of Homeland Security for 2012 is only $57 billion.[3]

President Obama's Cyber Space Review found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity"

Our companies are focused on providing a robust, multi-layered defense including extensive automated and business process controls with emphasis on deploying new analytical technologies that help us better understand threat indicators both on the inside of our network as well as our perimeter. We understand that basic security practices are necessary but not sufficient

---

[2] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.
[3] U.S. Department of Homeland Security. Department of Homeland Security Budget in Brief: FY 2012. Oct. 2011. Web. 6 Feb. 2012. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

for today's threats so we continue to explore new technologies to help identify and mitigate the Advanced Persistent Threat problem while investing in our workforce. We have developed strong relationships within and outside our sector to share information that leads to a more complete threat picture. We aggressively seek out best practices and share our own.

Despite the fact that our critical infrastructure is under constant cyber attack we have never had an instance of serious breakdown similar to what we have seen for example in the environmental arena.

This success is due in large part to the flexibility generated in the current system which relies on voluntary partnerships wherein industry, which understands and can manage these systems best, can use their intimate knowledge to respond to rapidly emerging cyber threats in a fashion they believe can best protect the system rather than being driven by a pre-set government requirement.

Nevertheless there is a great deal Congress, and the Commerce Committee, can do to assist to enhance our cyber security.

1. **Get their own house in order**

In addition to well know deficiencies from the WikiLeaks compromise to poor FISMA scores the National Academy of Sciences the GAO and just last week the DOE Inspector general have all documented systematic problems managing government cyber space. One immediate place to start is the consensus legislative FISMA reforms, which have been delayed for several years.

2. **Provide the right mix of regulation and incentives**

The evidence is overwhelming that the largest barrier to securing cyber space is economic. For industries where the economics of the industry are tied directly to a regulatory format, such as electric utilities, water, transportation, etc., the current regulatory structure can be used to motivate and fund needed cyber advancements.

For industries where the economics are not inherent to a regulatory structure, we need to motivate by providing appropriate market incentives to spur greater security investment. An excellent example of this approach is the

Rogers bill passed by the Intelligence Committee with broad bi-partisan support, which uses liability reforms to stimulate additional information sharing.

However, liability reform is one of many incentives that need to be unleashed to help secure our cyber networks such as:

- Greater use of government procurement
- Streamlined regulation in return for demonstrated security improvements
- Greater use of private insurance
- Streamlined permitting & licensing
- Stafford Act access

Incentive such as these can be used to stimulate investment, innovation and the adoption of security procedures beyond what is commercially viable.

This approach was advocated by the ISA in the Cyber Security Social Contract in 2008, President Obama's Cyber Space Policy Review in 2009, the Multi-trade association/civil liberties white paper on cyber security in 2010 and the House Task Force Report on cyber security in 2011.

A great deal of work needs to be done to fill out how these incentive models can be best deployed in the various sectors so that needed legislative changes can be made.

In the meantime, Congress ought to enact the FISMA reforms and information sharing bills I alluded to above, also strengthen our law enforcement criminal effort and improve the management of federal systems.

Passing this package of cyber reforms would be a historic---and politically achievable accomplishment.

Ladies and Gentlemen of the Commerce Committee.... what you are dealing with here is the invention of gun powder.... mandating thicker armor won't work just like building broader moats wouldn't stop invaders who had invented catapults, just like the Maginot line was no defense against the invading Germans in WWII.

Trying to use 19th & 20th century models & federally regulating the Internet will not be effective. We need a much more contemporary and creative approach wherein the private sector is engaged, not controlled by our government partners. We look forward to working together.

Written Statement of the Internet Security Alliance:

THE EVOLUTION OF THE CYBER THREAT AND THE NEED TO EVOLVE OUR UNDERSTANDING OF IT

THE EVOLVING CYBER THREAT

There has been a dramatic change in the cyber threat picture in the last 18-24 months.

Our main concerns are not "hackers" or kids in basements. The fact that a cyber system has been "breached" is no longer the metric that determines a successful cyber attack.

Cyber attackers have grown increasingly sophisticated. Not only are the tactics more complex but the number of individuals, organized groups, and nation states with these capabilities have also grown. In addition to the individual "hackers" that can do damage, we have groups of "hacktivists" that bring their political agendas from the physical world into the online world. These groups conduct denial of service attacks and trade in stolen information to push their message forward. We also see organized criminals and nation states that leverage sophisticated tools and inherent vulnerabilities in technology to gain long-term footholds on systems – this is commonly referred to now as Advanced Persistent Threat, APT.

The APT attackers are pros. They are highly organized, well-funded, expert attackers who use coordinated sets of attacking methods both technical and personal. The investment required to carry out these attacks suggests they are often nation-state supported.

Perhaps most indicative of these attacks, is that if they target a system, they will invariably compromise, or "breach" it.

We have seen these attacks for several years in the defense sector, although they have recently mitigated far more broadly. The most recent research shows that responding to APT style attacks has become the major focus in industries as diverse as utilities, consumer products, financial services, the industrial and manufacturing sector and even entertainment and media.

The most common current cyber threat uses a mixture of technology abuse (hacking), white collar (organized) crime techniques, and advertising expertise (phishing, spamming, social engineering, etc). With that mixture, criminal groups easily manipulate both human and machine weaknesses to gain access to items of value. Those items certainly include money and financial instruments, but also include intellectual property that can be sold. In fact, the entire motivation behind the APT-types of breaches is to steal information, not to cause disruptions. Current proposed cyber legislation is too focused on preventing terrorist-style disruptive attacks and not on preventing online criminal behavior.

While there is increased attention being paid to these ultra-sophisticated threats, traditional defenses are having a very difficult time keeping up with the evolving threat.

Companies are countering the APT principally through virus protection (51%) and either intrusion detection or prevention solutions (27%).[4]

However, "Conventional information security defenses don't work vs. APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated."[5]

This doesn't mean we have no defense. It does mean we need to modernize our notion of what constitutes cyber defense. Traditional approaches, including federal regulation will not solve the problem as it will be largely reactive and not stay ahead of the changing nature of the threat. Worse, bad regulation could be counter-productive, leading companies to expend their limited resources on building in-house efforts to meet regulatory demands over actually dealing with the threat proactively.

ECONOMICS: THE MAJOR OBSTACLE TO PROVIDING CYBER SECURITY

Fundamental to stopping the advanced cyber threat is understanding that our biggest problems are not technological, but economic.

---

[4] PricewaterhouseCoopers. "Global State of Information Security Survey: 2012." Sept. 2011.
[5] Mandiant. Mandiant M-Trends Report 2011. at p.2. Jan. 2011. Web. <http://www.security.nl/files/M-trends2.pdf>

It is short sighted to think of the cyber threat as simply a technological issue that can be solved through standards and performance requirements. In reality the cyber threat is much more complex with as many strategic, human and economic issues as operational and technical ones---yet many of the current government actions and new proposals focus almost entirely on operational and technical issues when the real issue is economic.

Independent research has continually born out the fact that security flaws stem as much from poor incentives as they do from bad technological design.[6] In cyber security the current economic incentives all favor the attackers. Attacks are cheap & profitable while defense is expensive, difficult to justify with economic ROI and criminal prosecution is almost non-existent---less than 1%.

Research from Pricewaterhouse, CIO Magazine, CSIS & McAfee as well as ISA's own work has consistently shown that the single biggest problem in combating cyber threat is not technical, but is cost.[7],[8],[9] Several of these studies also document that although the threat is increasing, spending on cyber security has been reduced between 50%-66% of American companies over the past few years.[10],[11]

Just last week, Bloomberg released an extensive study that found to reach an acceptable, not the ideal, level of security in critical infrastructure would require a 91 percent annual spending increase.

"In general, organizations recognize that they are very, very vulnerable, and they don't actually have enough resources to get the job done properly," said Larry Ponemon, who conducted the study for Bloomberg.[12]

---

[6] Ross Anderson and Tyler Moore, "The Economics of Information Security: A Survey and Open Questions." *Science*, Vol 314, #5799, American Association for the Advancement of Science, Washington DC. 27 Oct. 2006

[7] PricewaterhouseCoopers. The Global State of Information Security: 2008.

[8] "Business Partners with Shoddy Security; Cloud Providers with Dubious Risk Controls; What's a CIO to Do?" CIO Magazine. Oct. 2010.

[9] McAfee and Center for Strategic & International Studies. In the Crossfire: Critical Infrastructure in the Age of Cyber War. 2010.

[10] McAfee and Center for Strategic & International Studies. In the Crossfire: Critical Infrastructure in the Age of Cyber War. 2010.

[11] PricewaterhouseCoopers. "Global State of Information Security Survey: 2010."

[12] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Bloomberg Government Study, 31 Jan. 2012.

WHAT IS THE PRIVATE SECTOR DOING?

The private sector has been extremely responsive to combating the cyber threat on several different levels. The private sector has been extremely responsive to combating the cyber threat. Private sector spending by US companies on cyber security has doubled in the last 5 years and is projected to be approximately 80 billion dollars for 2011[13] ---- by comparison, the official spending request for the entire Department of Homeland Security for 2012 is only $57 billion.[14]

The Market has Developed Effective Cyber Security Programs

The private sector has been aggressive in continually innovating and creating standards practices and technologies to counter the cyber threat.

For more than a decade, the ISA and its member companies have been engaged in thought leadership and creating and operating programs designed to enhance our nation's cyber security. Among the programs the ISA has initiated and operated in conjunction with our partners are programs on Enterprise Risk Management, Information Sharing, Insider Threats, Mobile Security, Senior Management Education, Supply Chain Management, Small Business and Home User Security and best practices to help combat the Advanced Persistent Threat.[15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25]

---

[13] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.
[14] U.S. Department of Homeland Security. Department of Homeland Security Budget in Brief: FY 2012. Oct. 2011. Web. 6 Feb. 2012. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.
[15] Internet Security Alliance and the American National Standards Institute. "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask." 2008.
[16] Internet Security Alliance and the American National Standards Institute. "The Financial Management of Cyber Risk: An Implementation Framework for CFOs." 2010.
[17] Internet Security Alliance, paper by Jeff Brown, Raytheon Company, entitled "A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels," March 2009.
[18] Internet Security Alliance. "Common Sense Guide to Prevention and Detection of Insider Threats - 1st Edition." 2005.
[19] Internet Security Alliance. "Common Sense Guide to Prevention and Detection of Insider Threats – 2nd Edition." 2006.
[20] Internet Security Alliance. "Common Sense Guide to Prevention and Detection of Insider Threats – 3rd Edition." 2008.
[21] Internet Security Alliance. "Applicability of SCAP to VoIP Systems." 2010.
[22] Internet Security Alliance. "Common Sense Guide for Senior Managers." 2002
[23] Internet Security Alliance. "ISA Guidelines for Securing the Electronics Supply Chain." Publication forthcoming.
[24] Internet Security Alliance. "Common Sense Guide for Small Businesses." 2004.
[25] Internet Security Alliance. "Common Sense Guide for Home and Individual Users." 2003.

Although the ISA opens its programs and projects to government participants, it receives no government funding. All ISA programs are supported by voluntary contributions from the private sector. All ISA products and services are available on an open source model and free of charge to all consumers.

The ISA and its members compromise only a small fraction of the investment made by the private sector to secure our overall system. Moreover, industry, and governmental analysis has demonstrated that, if these systems were implemented they would yield substantial success.

Verizon in conjunction with the US Secret Service has done a series of studies in which they performed a forensic analysis of hundreds of successful cyber breaches, analyzing tens of thousands of data points. The research has documented that had the organizations who suffered the breaches followed standards and practices already existing in the market, they would have prevented or mitigated mitigate the effects of up to 94% of cyber attacks.[26]

Shortly after taking office, President Obama commissioned the National Security Council staff to review our nation's effort in cyber defense. Their report, "The Cyberspace Policy Review"[27] found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."

Although it is well known that neither the public nor private sectors have been successful in stopping all cyber attacks, we have been successful in preventing our critical infrastructure systems from being seriously compromised.

For example, several of the major bills being considered in Congress, including that approved in the House Cyber Subcommittee of HLS and the circulating Senate drafts address cyber attacks of high national significance, i.e., ones that would result in "interruption of life sustaining services

---

[26] Wade Baker et al., "2010 Data Breach Investigations Report" Verizon Business, 2010. <http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf>.
[27] Obama Administration. "Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure."

sufficient to cause, mass casualty ... mass evacuations ... catastrophic economic damage or severe degradation of our national security." No less an authority than Homeland Security Secretary Napolitano has asserted that our critical infrastructure is under cyber attack thousands of times a day, which translates into hundreds of thousands of times a year and millions of attacks in just the past few years.[28]

Despite this environment of constant cyber attack, however, there has never been a single instance of cyber attack even approaching the level the bill's draft addresses. This success in protecting our critical infrastructure, while not perfect, is due in large part to the flexibility generated in the current system which relies on voluntary partnerships within industry, which understand and can manage these systems best. These partnerships can use their intimate knowledge plus information provided, at times by the government, to respond to rapidly emerging cyber threats in a fashion they believe can best protect the system.

Federal Mandates Could Compromise Cyber Security

This ability to be responsive to the situation on the ground, without having to worry about complying with a pre-set federal requirement is especially critical in the cyber security space wherein infrastructure owners and operators need to be responsive to novel situations which evolve constantly. In such instances, it is critical that owners and operators dealing with a major attack are focused first and foremost on what needs to be done to mitigate the attack, and not the reading of a pre-set performance requirement.

For example, it might be assumed that performance requirements would be set at such a level of generality that they will not impede the managing of an attack. However, even steps that were a few years ago obvious, such as securing the perimeter or stopping the attack as soon as possible, have now been shown to be either impractical (as in the case of the former) or unwise (as often in the case of the latter). In this rapidly changing environment, incentives to undertake the most effective measures, rather than requirements to follow the government mandate are what we need to be creating to secure our cyber systems.

---

[28] Napolitano, Janet. "Cybersecurity: Protecting Our Nation's Assets," Washington Post Live, Washington, D.C.. 27 Oct. 2011. Web. <http://washingtonpostlive.com/conferences/cybersecurity>.

Moreover, one of the characteristics of the APT is that attackers will virtually always succeed in successfully breaching the targeted cyber system. As a result, a "performance requirement," such as maintaining a breach proof environment may be, in the current context, hopelessly unrealistic and investment toward that end may well be an inappropriate use of scarce cyber security resources.

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

The kinds of language and administrative formulas that would have to be adopted to comply with the proposed requirements would almost certainly have little to do with real cyber security. This is partly because the field is developing so rapidly that by the time cyber security "requirement" were recognized as fulfilling administrative expectations, it would already be obsolete. There is also no way to tell at the level of a "general requirement" whether the cyber security measures involved would be doing any good or not.

The resources required to address the types of attacks we are concerned with here need to be, as they currently and successfully are, based on expert analysis on the ground, not a federally predetermined standard or requirement.

Major Enterprises are Aggressively Pursuing Cyber Security

Finally, at a enterprise level we are focused on ensuring a robust, multi-layered defense including extensive automated and business process controls with emphasis on deploying new analytical technologies that help us better understand threat indicators both on the inside of our network as well as our perimeter. We understand that basic security practices are necessary but not

sufficient for today's threats so we continue to explore new technologies to help identify and mitigate the Advanced Persistent Threat problem while investing in our workforce. We have developed strong relationships within and outside our sector to share information that leads to a more complete threat picture. We aggressively seek out best practices and share our own.

Maintaining the current rate of success in stopping catastrophic cyber attacks, and expanding this success to other sectors will require us to directly address how we finance solutions. The notion that a large complex and serious problem can be easily and cheaply solved with a new government mandate defies common sense.

WHAT SHOULD THE GOVERNMENT BE DOING?

Notwithstanding that there is already excellent work being done to secure cyber systems, ISA believes, and has believed since its inception in 2000, that the federal government can and should be doing more to assist in our cyber defense. Specifically, the federal government needs to get its own house in order, provide the right mix of incentives and regulations to the private sector and, above all, do no harm.

3. Get their own house in order

Congress' role in cyber security needs to centered on leadership rather than law-making. Via Congress' oversight and appropriations responsibilities, the federal government's own networks should be built and operated to world-class standards in terms of security and should set the example for others to match. By setting the bar high for government networks and encouraging state and local governments to follow, industry will find it easier to purchase and install solutions that are already proven to work on government networks. This has the dual advantage of driving new jobs in the technology sector via increased federal spending on cyber security product development and acquisition; and it will push security technology innovation into new areas that might not be reached if left to traditional market forces.

Unfortunately, government has not matured its own cyber processes sufficient to be placed in the position of judging industry's management of the far more diverse systems in the private sector.

For example, the damaging WikiLeaks compromise last year was not a sophisticated attack but the result of rudimentary organizational mismanagement. Moreover the governments own low FISMA scores attest to the need for the government to improve its own management systems and there are numerous other recent examples of the need to mature the federal management systems including:

National Academy of Sciences review of DHS cyber consequences found that they were missing critical elements:

"DHS analyses of consequences have tended to focus on the outcomes that are most readily quantified. Little attention has been paid to secondary economic effects or to an attack's effects on personal and group behaviors—impacts that could be significant and may be the primary goals of terrorists. Some relevant research is being conducted in DHS...but much more is needed. In addition, efforts must be made to incorporate the results of such research into DHS risk analyses and to heighten risk analysts' awareness of the importance of social and economic impacts."

With respect to DHS risk management capability the national Academy found "it is very difficult to know precisely how DHS risk analyses are being done and whether their results are reliable and useful in guiding decisions."As recently as December 9, 2011 the GAO criticized DHS and other federal agencies for its failures to adequately promote **effective** cyber security measures in its report, entitled "Critical Infrastructure Protection: Cyber Security Guidance Is Available, but More Can Be Done to Promote Its Use," GAO found that:

> "Implementation of cyber security guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, sector-specific agencies could take additional steps to promote the most applicable and effective guidance throughout the sectors . . . Federal policy establishes the dissemination and promotion of cyber security-related standards and guidance as a goal to enhancing the security of our nation's cyber-reliant critical infrastructure. DHS and the other lead agencies for the sectors selected for review have disseminated and promoted cyber security guidance among and within sectors. However, DHS and the other sector-specific agencies have not identified the key cyber security guidance applicable to or widely used

> in each of their respective critical infrastructure sectors. In addition, most of the sector-specific critical infrastructure protection plans for the sectors reviewed do not identify key guidance and standards for cyber security because doing so was not specifically suggested by DHS guidance. Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets...GAO is recommending that the Department of Homeland Security (DHS), in collaboration with public and private sector partners, determine whether it is appropriate to have cyber security guidance listed in sector plans. DHS concurred with GAO's recommendation."

Just last week it was reported that the Department of Energy's Inspector General had found that the Department's rush to award stimulus grants for projects under the next generation of the power grid, known as the Smart Grid, resulted in some firms receiving funds without submitting complete plans for how to safeguard the grid from cyber attacks, according to an inspector general's report.

"Officials approved cyber security plans for Smart Grid projects even though some of the plans contained shortcomings that could result in poorly implemented controls," states the report. "We also found that the Department was so focused on quickly disbursing Recovery Act funds that it had not ensured personnel received adequate grants management training." According to the report, 36 percent of the grant applications submitted were lacking one or more elements in their cyber security plans. Three out of the five cyber security plans reviewed by the IG were incomplete, and often didn't address weaknesses previously identified by the Energy Department.

It would seem obvious that before Congress granted extended power to the government to make cyber security decisions for the private sector it ought at least to demonstrate they can manage this task for their own, comparatively limited systems

4. Provide the proper mix between incentives regulation and incentives

It's obvious neither government nor industry can alone address the growing cyber security issues.

In 2008, ISA proposed an alternative model, a cyber security social contract wherein government would provide market incentives to cover the investments required for industry to take on additional cyber security defense.

In 2009, when President Obama released the Cyber space Policy Review based on a in-depth study by the National Security Council staff the Executive Summary both began and ended by citing the ISA Social Contract The President's document which specifically urged the consideration of several such market incentives.

In 2010, a coalition of 5 industry and civil liberties groups adopted a similar set of recommendations.

In 2011, the House Republican Task Force adopted as its very first recommendation that congress needs to develop a menu of market incentives to address our collective cyber security problems.

In 2012, we hope to see legislation, such as Congressman Roger's bill, which uses liability protections as an incentive to spur greater information sharing to reach the House floor.

The Rogers bill does more than simply providing a tangible incentive to share information, it signals a more progressive approach to the government industry relationship which moves in the direction that will generate increased cooperation.

Classification, breach disclosure laws, SEC regulations and the like all have their place, but they also have the unintended consequence of inhibiting sharing because they create an atmosphere wherein having information to share is presumed to be indicative of a breach that must be disclosed. What it should be is a celebration that someone has valuable information to share without any question as to how they found it. It is reflected in government language of wanting companies to report compromises when they should be

asking industry to report indicators. It is a subtle difference but the former is seen as a confession that risks punishment (official or in the press) while the later is seen as a measure of the skill of the reporting company

The private sector takes cyber security very seriously and is spending a good percentage of their IT budgets on protecting their networks and digital property from relentless criminal attacks. However, the private sector is held back by old laws that discourage the rapid sharing of timely information, and by a general reluctance of local law enforcement organizations to provide the training and advice on how to be secure in cyberspace the same way that information is readily made available for physical security. The private sector needs help, but they don't need additional regulation. Remove the old barriers to rapid information sharing and beef up the capabilities of local law enforcement organizations to "take a byte out of crime" in the digital world.

However, there is a great deal more that needs to be done In addition, to liability incentives there are wide ranges of additional incentives that are low cost to the government but could create powerful incentives to promote additional critical infrastructure security on a sustainable basis. These incentives include:

- Greater use of government procurement
- Streamlined regulation in return for demonstrated security improvements
- Greater use of private insurance
- Streamlined permitting & licensing
- Stafford Act access

This approach is also consistent with the Administration's policy for establishing regulations as articulated in Executive Order 13563, January 2011, which directs agencies to "identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public."

5. Do no harm

ISA has been lobbying for greater government attention to our cyber security problems for over a decade and so we are naturally grateful to see legislation moving to address this problem.

However, there is a difference between realizing that there is a significant problem and developing an effective and comprehensive solution.

Some, surely well intentioned, proposals, not only bear little hope of addressing the issue but run the risk of making things much worse.

No less an authority than the current Deputy Undersecretary for Cyber Security at DHS, Mark Weatherford, has noted the potential danger of moving in this direction:

"As I study [recent] pieces of [cyber security] legislation, the one thing that concerns me is the potential negative implications and unintended consequences of creating more security compliance requirements. Regulation and the consequent compliance requirements could boost costs and misallocate resources — without necessarily increasing security due to placing too much emphasis on the wrong things. It is therefore critical that any legislation avoids diverting resources from accomplishing real security by driving it further down the chief security officer's (CSO's) stack of priorities."

The notion that all we need is a set of federal regulations is vastly over simplified----and potentially dangerous.

Blaming the victims of cyber attack is unjustified, unfair and unhelpful.

Ladies and Gentlemen of the Commerce Committee....what you are dealing with here is the invention of gun powder....mandating thicker armor won't work just like building broader moats wouldn't stop invaders who had invented catapults, just like the Maginot line was no defense against the invading Germans in WWII.

We can't use 19th & 20th century models, federally regulating the Internet, or giving DHS the power to make the final decisions about securing technology they don't own or operate; they will make our cyber security less effective.

We need a much more contemporary and creative approach wherein the private sector is engaged, not controlled by our government partners. We believe the Task Force Report goes in the right direction and urge you to follow that approach.

Mr. WALDEN. Mr. Clinton, thank you very much for your testimony. We appreciate it.

Our next and final witness today is Phyllis Schneck, who is Vice President and Chief Technology Officer of the Global Public Sector, McAfee Incorporated. Dr. Schneck, thank you for being here today. We look forward to your comments.

STATEMENT OF PHYLLIS SCHNECK

Ms. SCHNECK. Good morning, Chairman Walden and Ranking Member Eshoo and other members of the subcommittee. Thank you very much for the opportunity to be here this morning, and thank you for your interest in cybersecurity as it applies to the telecom sector.

My testimony will focus this morning on four areas: the threat landscape, the communications sector's unique role in cybersecurity, private sector technologies and policy recommendations to enable greater cross-sector cyber resilience.

First, just a bit of background. My technical background is high-performance computing and cryptography. I was raised in this back to the days of the radio tower. My father was one of the first in supercomputing in this country and taught me to write code. I know how to exploit code, but I was taught the responsibility of that and the responsibility of the computing power that we have and I am confused on and passionate about protecting that and protecting good science. I am also focused on partnership. Outside of McAfee as a volunteer, I ran the private sector side of the FBI's InfraGard program, about which Director Mueller testified several times. I ran that for 8 years and grew that program from 2,000 subject-matter experts across the critical infrastructure sectors to 33,000, and today chair the national board of directors for the National Cyber Forensics and Training Alliance, which brings together the top fraud analysts from the banking sector, telecom, pharmaceuticals, and others with the FBI under the same roof and other organizations and governments, do analytics that helped to arrest 400 cyber criminals worldwide in the past 2 years.

A little bit about McAfee. We are based in Santa Clara. We are the world's largest dedicated security company. We protect business, governments and consumers all over the world from the full spectrum of cybersecurity attacks. We are a trusted partner and adviser on cybersecurity throughout the world, and as a wholly owned subsidiary of the Intel Corporation enjoy driving that innovation that goes directly to the hardware. The buck stops at the hardware, so the adversaries can get in in several different ways, but when a piece of hardware knows not to execute a malicious instruction, that is when we have the enemy.

As you have heard this morning, the cyber threat landscape has evolved. Obviously it is not a dorm-room activity anymore. It is more a mass espionage. There are two kinds of companies and agencies across the world, public sector and private, those who know they are owned and those who don't. We are looking at the mass movement of money markets and jobs between countries and companies and we are looking at the threat of destruction should they desire. This enemy is faster and smarter than we are at times. They are certainly faster. They have no intellectual property

boundaries, no legal boundaries, no policy boundaries, and in many cases, they have plenty of money. They have absolutely no obstacles to execute on our infrastructure.

Which leads us to the role of the Internet service providers. In the days when I sent my first packets between my sister's room and mine, there was nothing in that route except one address on the other. Now we have an unknown set of routes but we have an ability and a great infrastructure run by the ISPs that deliver our traffic and that of the adversary very reliably. So the enemy has now used our great cyber infrastructures that we built as the good guys over the world as a mass executive transport system for malware. They haul packets at high speed. They do a great job. They are fairly secure, as was mentioned earlier, but the current Internet architecture allows everything to get delivered to the grid, to the banks, to the rest of the critical infrastructure.

ISPs can play a key role in better cybersecurity. They are already doing some of this but they have some challenges. One thing they can do is help detect this traffic in the network fabric and use some global threat intelligence to do that, and I will explain that in just a moment, but imagine if our network fabric was smart enough not to route the traffic of an adversary and only to route good traffic. Secondly, demand more secure technologies and equipment from the market. Demand that those technologies are armed with proactive technologies and not let a malicious instruction run. And third, ISPs can't carry the burden alone. As was said earlier, it is up to every system to be hardened, up to every company and user to harden their enterprise, and good cyber hygiene plays a role in that.

What are the challenges that the ISPs face today? Just to name a couple, you have things such as Stored Communications Act of 1986, a little while ago. That was before I sent my first packet. It prevents sharing information outside of the telecoms, so imagine the difficulty in enabling the global threat picture that the enemies use. We can't make that rule because legally we can't combine our information together. Secondly, it costs a lot of money. Clean bandwidth costs money and users aren't willing to pay that difference, so we need some help leading to some policy recommendations and some proactive technologies.

First and foremost, we can put threat intelligence together and map a global cyber radar map of where the enemy is at any time. At McAfee, across 160 million endpoints, we see a risk profile in every IP address on the Internet. Other companies do this. Telecoms do this. Governments can do this if we can share that information together and make a global threat picture and prevent those malicious instructions from running, whether it is application listing or working with the hardware, keep the enemy out.

So for the policy recommendations, we support the recommendations in Representative Thornberry's work, certainly with information sharing, insurance reforms and tax credits, and certainly in the bill of Representative Rogers and Representative Ruppersberger enabling the government to finally facilitate the good information sharing, to put that information together to not only provide liability protections, protections for privacy and for civil liberties, but to balance out the advantage that the adver-

saries had over us until now. Let the government facilitate that collaboration so we can build that global threat picture, feed it back into the network fabric, and have it grow as a living, breathing system to feed us the information in return. ISPs play a central role in the global digital infrastructure. They can help us. We can help them. We have to work on this legal and policy framework for global information sharing.

Thank you very much for requesting McAfee's views on these issues. I look forward to answering any questions.

[The prepared statement of Ms. Schneck follows:]

STATEMENT OF

DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, PUBLIC SECTOR,

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

"CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND PRIVATE-SECTOR RESPONSES"

FEBRUARY 8, 2012

Good morning Chairman Walden, Ranking Member Eshoo, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer-Global Public Sector for McAfee. We appreciate the Subcommittee's interest in cyber security as it affects the communications sector, as well as your interest in the private sector's response.

My testimony will focus on the following key areas:

- Today's cyber security threat landscape
- The communications sector's unique role in cyber security
- Private sector technologies such as Application Whitelisting and Global Threat Intelligence that are reducing the profit model of the cyber adversary
- Policy recommendations to encourage public-private sector information sharing at both human and machine speeds -- essential for responding to the modern cyber security challenge

First I would like to provide some background on my experience and on McAfee.

I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to my role with McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 400 cyber criminals

worldwide. Previously, I served as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence, a system of real-time risk indicators. I have also served as a Commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (CSIS) Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program, building our relationships between FBI, DHS and other organizations and growing the InfraGard program from 2,000 to over 33,000 members nationwide. Prior to McAfee, I served in several executive roles in the security industry and also started and sold a business of my own in the security space. I also worked for several years at the MITRE Corporation in telecommunications network pricing algorithms. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 150 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Today's Cyber Security Threat Landscape

We face a transnational cyber adversary that is smart, fast, and has no legal, intellectual property, international or competitive boundaries. This adversary is often well funded, with no impediments to swift execution, and one of the most

effective ways to defeat this adversary is through the light speed communications infrastructures owned and operated by the Internet Service Providers (ISPs).

The cyber security threat landscape has changed fundamentally over the last decade as cyber threats have become increasingly more sophisticated and targeted. What had been science fiction is now reality: malicious actors perpetrating cyber attacks that steal money and intellectual property, disrupt businesses, sabotage critical infrastructure, and/or threaten governments and nation states. In fact, the past few years have demonstrated the largest known movement of money, markets, and jobs between countries and companies, all facilitated by cyber intrusions. Because global cyber connectivity enables all of this activity, it creates difficulties for attribution and punishment. This must change. A recent report McAfee released in conjunction with the Security & Defence Agenda (SDA), the leading defense and security think-tank in Brussels, found that 57% of global cyber security experts believe an arms race is taking place in cyber space, and 45% believe cyber security is as important as border security. Many governments around the world – including the U.S. – have acknowledged that cyber threats can be every bit as menacing as physical threats to a nation's security, and the U.S. military, for example, has declared cyberspace a realm that warrants protecting.

McAfee Labs' most recent threat predictions include an increase in attacks on smartphones and mobile devices. Attackers have moved on from simple destructive malware to spyware and malware that makes them money, exploiting vulnerabilities to bypass system protections and gain greater control over mobile devices. Researchers also predict that 2012 will see a move toward mobile-banking attacks.

Not only the kinds of attacks but the kinds of attackers have evolved as well. Cybercrime perpetrators have morphed from simple, low-budget hackers into well-financed criminal operations that contribute to a multi-million dollar cybercrime industry. Not all cybercrime has a financial incentive, however. Cyber criminals now include those interested in stealing intellectual property, personal/professional information and state secrets, gaining access to a nation's entire slate of cyber processes, compromising critical infrastructures, advocating a cause ("hacktivism"), and/or launching a terrorist attack.

By leveraging multiple threat vectors, hackers are able to extend the time period in which their malware remains undetected and are able to steal the money, personal data, and other valuable information of users throughout the United States and the world. In this way, what might be called classic "viruses" have been blended in recent years with other types of malware and techniques used by malicious hackers intent on stealing personal data. Hackers have discovered that direct external attacks are unnecessary and risky. It is now easier to engineer malicious software that is delivered to a system remotely through various means and that can insidiously send information back to hackers indefinitely before being detected.

Modern malware, therefore, can no longer be classified by its perceived purpose or propagation method, because both can change in an instant. Some types of software can be engineered to gain access to and maintain control over a victim's machine. Once the malware is on the system, it seeks to communicate with its controlling entity – the criminal actor. And once communication is established over the Internet, any compromised machine can be instructed both to pass over any data of value to the criminal and to act as an instrument of attack against other computers and networks.

Today, malware developers combine web, host, and network vulnerabilities with spam, rootkits (invisible malware that hides within authorized software in a computer's operating system), spyware, worms (which target computers rather than software programs but which can clog communications bandwidth and overload computers or networks,) and other means of attack. Malware also can be distributed indirectly by networks of computers that have been corrupted by a criminal – known as a "botnet," or a collection of compromised computers connected to the Internet.

Then there is the type of attack known as an Advanced Persistent Threat (APT), which is essentially an insidious, persistent intruder meant to fly below the radar screen and quietly explore and steal the contents of the target network. In the past two years, McAfee has uncovered numerous APTs affecting tens of thousands of organizations worldwide. Three of these large scale but quiet espionage operations drew particular attention – Operation Shady RAT, Operation Aurora, and Night Dragon. These attacks are significant because they were managed by coordinated, organized teams that succeeded in extracting billions of dollars of intellectual property from leading global companies in the information technology, defense, and energy sectors – strategic industries vital to any country's long-term economic success and national security. These low-profile attacks are often more dangerous than the high-profile incursions because they are a type of cyber espionage, providing silent, ongoing access to protected institutional information. And these APTs are not limited in scope; they can affect any company, government body or nation, regardless of sector, size, or geography.

The Communications Sector's Unique Role in Cyber Security

ISPs are foundational to all electronic communications activity. As such, they depend on hardware and software vendors to supply highly secure products and services to ensure that their systems are protected from a wide variety of attacks, particularly APTs. ISP's have, and will continue to demand that their vendors supply them with ever more secure products and services.

We also believe that ISPs can work even better with more situational awareness and a greater ability to correlate events within and beyond their own data. They can influence the market through the acquisition of systems and technology innovations

that address resiliency through blocking the execution of malicious instructions, as we describe later in this testimony. Finally, ISPs cannot carry the burden alone, and all systems should follow these premises. Cyber resiliency assumes the adversary will get in and that this will not be detrimental. This assumption can only be realized in a system that can detect and deter malicious instructions.

Internet Service Providers form the literal backbone of global communications. All Internet traffic is enabled at some point by an ISP – even the traffic of the malicious actors. Since ISPs haul the packets, it is the hope that others in industry can partner with ISPs to enhance technology and policy so as to eventually prevent the enablement of cyber adversaries, as well as to harden the ISPs and CIKR (Critical Infrastructure and Key Structures Resource Center) even further.

It's not just businesses, organizations and individuals who are at risk, of course. The cyber risk to our nation's critical infrastructures is real, and fortunately, policy makers are becoming more aware of the need to protect such vital systems as energy, water, transportation, and finance from cyber incursions. The communications sector is unique among critical infrastructures, however, in that it is the delivery mechanism for voice and data – including data from malicious actors. The Internet was architected to ensure that information arrives at the destination specified by its sender. Therefore, the Internet currently ensures the delivery of malware, leaving the receiver responsible to identify and prevent entry and/or damage from the malicious instructions upon arrival. Criminal actors, whether abusing the networks with botnets and other unsavory activity, or simply communicating, rely on communications networks just as much as law enforcement agencies checking a suspect's record in a federal database. Thus high-speed communications networks and ISPs become the agnostic enablers of both sides of the Information Age's equation.

Telecommunications companies are no strangers to network security practices. For years they have been working to keep their networks robust and secure. But the universe of online players is now so vast and interconnected, and the cyber threat is growing so rapidly, that even more is required. ISPs are under continuing pressure to provide "clean pipes," a term used often in the industry for the delivery of traffic that has been "cleaned" of potential threats. From a strictly technical perspective, many ISPs have the ability to detect threats and remove some from the traffic before it is passed on. They could technically also check that routes have not been modified. However, when one considers other factors– such as cost, customer attitudes toward privacy, and ISP liability – the right answer is neither clear nor simple, especially at speeds of hundreds of gigabytes per second between ISPs and users.

The prize goal is to remove dangerous traffic instead of ensuring its arrival at its sender-specified destination. However, this requires several additional steps, such as global situational awareness, enabling the legal and policy framework, and a business case with clear return on investment.

ISPs and other telecommunications providers currently confront a wide array of federal, state, and international regulations that complicate their task of cleaning the pipes. The *Stored Communications Act of 1986*, for instance, often prevents ISPs from disclosing information about communications outside of their organization. This is just one example of a complex web of rules that have the effect of creating an environment of disincentives for ISPs and other telecommunications providers to collaborate with security companies in addressing the cyber security challenge.

ISPs are also confronted with financial disincentives that limit their ability to address this challenge. According to a major study done by the Institute for Homeland Security Studies, "An Economic Analysis of ISP Provided Cyber Security Solutions," most customers are willing to pay only $5 extra per month to receive an appropriate level of security. Thus ISP firms are forced to work within very tight margin constraints. Their customers are willing to pay a small amount to protect their own data but are not willing to pay extra to address the larger, structural security challenge: the reality that cyber attackers abuse the network to inflict attacks on a wide variety of targets.

This is a classic commons problem, and thus it is appropriate for government to work to address it, given governmental interest in reducing the threat of cyber attacks on the entire system. The types of positive incentives put forth by the ISP community – the types of positive incentives that we, too, support – do in fact make sense and are entirely appropriate for policymakers to consider. The entire Internet eco-system – from the core of the network to the enterprise edge to the individual systems and hardware, from ISPs to users, from the government to private sector experts – needs to be involved to combat the growing cyber threats that we as a nation face.

Private Sector Innovation: Two Proactive Technologies

The good news is that innovation in the private sector is vibrant, and is enabling security providers to address APTs, botnets and other incursions. Leading information technology companies and their customers are uniquely positioned to act as early warning systems that can identify and help address cyber security attacks as a real-time cyber immune system. Information technology companies focused on cyber security, in particular, have the resources and the economic incentives to continue to invent and develop the technologies and solutions needed to stay ahead of sophisticated cyber attackers.

Two of these technologies are application whitelisting and Global Threat Intelligence. Both represent a new paradigm in cyber defense in that they are proactive and predictive, respectively, rather than reactive.

Application Whitelisting – Preventing the Execution of Malicious Instructions

The concept of application whitelisting flips the traditional antivirus model from one that identifies and attempts to block all malicious code (a concept known as blacklisting) to one that understands that the adversaries will get in but can be prevented from executing. This technology allows only good, pre-approved code to enter a system. Whitelisting instructions reside at the operating system level and simply do not permit the execution of any instruction set that has not been previously approved. Technologies based on whitelisting allow organizations to identify in advance only the software and executables that are permissible for downloading and executing on their systems. All other applications, such as malicious software, are denied by default.

Thus, even though the adversary may in fact be able to get malicious code onto a machine, that machine, if equipped with whitelisting technology, will never execute the malicious instructions. The analogy in biology is exposing a person to a disease that will never be able to develop or harm the person. The germ remains dormant, as do the malicious instructions in a machine protected by application whitelisting. Whitelisting technology enables organizations to be much more proactive in protecting their systems. The technology is used to protect servers, endpoints, embedded devices and mobile devices. Significantly, whitelisting can also protect the integrity of many ATMs, point-of-sale terminals, and Supervisory Control and Data Acquisition (SCADA) systems, which, because of CPU and performance resource constraints, often might not support traditional anti-malware software.

Global Threat Intelligence – Helping ISPs to Not Route the Traffic of the Adversaries

McAfee and other sophisticated cyber security providers have developed a technology that is unique in that it is predictive and not reactive. It enables multi-vector, real-time, predictive protection against the more sophisticated attacks on information systems. McAfee's solution is called Global Threat Intelligence, or GTI. GTI is the basis of a cyber immune system: the ability to protect against an attack by electronically detecting and correlating, at machine speed, cyber behavioral data from worldwide sources that is identified as harmful – long before a traditional anti-virus "signature" or name might be developed at human speed. The biological analogy is the human body defending against a potential disease simply because the body detects that the behavior is harmful.

McAfee's GTI uses 160 million sensors to span the Internet, continually seeking and identifying new and emerging threats before they materialize. To interpret this data, McAfee dedicates more than 350 researchers in 30 countries to focus exclusively on tracking and analyzing threat information, providing the most relevant security information 24x7. For instance, through global sensors researchers can note the prevalence of a new behavior and its propagation pattern and pace as it progresses through different countries, different types of users, or different delivery mechanisms. In milliseconds, GTI can assess changes, assign risk levels, and

distribute protection recommendations to products covering every threat at every tier.

Cyber security solutions based on this GTI approach protect computers by calculating the potential risk of a piece of content based on experience with either the IP address from which it originates, the website, or other elements associated with the content in question. Thus solutions can be offered that enable customers to be warned that, in the GTI provider's view, the content is too risky to be loaded into the memory of their computer.

ISP's currently address certain botnets with traffic flow data, but only those botnets that the ISP can see with the cyber intelligence they have. Collecting data from multiple sources would enhance the situational awareness picture and allow those who transport our traffic to see botnets that may be too dispersed to be noticed immediately with conventional traffic flow data. When used effectively, GTI technology can prevent the routing of traffic from bots and/or assist with the identification of infected machines that may be customers of the ISP, allowing the ISP to explore ways to help those customers clean the malware off their systems.

Technologies such as GTI – and others that are just now being developed – can actually decrease the profit model for cyber criminals across the spectrum, from the hacker hobbyist to the espionage or APT players. There is often overlap in the infected resources used, and application of collaborative GTI from multiple sources at the ISP can reduce the malicious traffic that is routed, leaving an Internet that is no longer a reliable transport system for danger. This is one reason McAfee believes that any national cyber security plan must involve the private sector – not just at the beginning, but at every stage.

Policy Recommendations

In general, we believe that positive incentives are superior to regulation in achieving the desired national outcome: a cyber secure nation. Using positive incentives rather than negative ones, such as government mandates, is the most effective way to drive higher levels of trust and actual cooperation between the private sector and government – all vital to producing real success.

Fortunately, we are not starting from scratch. There are a variety of approaches focused on positive incentives in play. Many of the recommendations of Representative Thornberry's (R-Texas) Cyber Security Task Force are a step in the right direction in that they address a wide range of incentives such as information sharing, insurance reforms, and tax credits. And over the past few years there has been good bipartisan collaboration on a number of cyber initiatives, including additional investment in cyber security research and FISMA reform, to name just a few.

In this same spirit, the information sharing bill introduced by Representative Mike Rogers (R-Michigan) and co-sponsored by Representative Dutch Ruppersberger (D-Maryland), the *Cyber Intelligence Sharing and Protection Act of 2011* (H.R. 3523), would be particularly effective in encouraging the kind of public-private partnerships we need to move forward in cyber security. An amended version of this bill passed the House Intelligence Committee in December with overwhelming bipartisan support. The premise of the bill matches our own on this issue: that government can facilitate collaboration and encourage trusted working relationships to the benefit of all parties in the Internet ecosystem.

H.R.3523 gives the federal government new authority to share classified cyber threat information with approved companies so they can better protect themselves and their customers from cyber attacks. The bill also empowers participating businesses to share cyber threat information with others in the private sector and enables the private sector to share information with the government on a voluntary basis. Importantly, the legislation also provides liability protection for companies that choose to protect their own networks or share threat information. Equally important, the bill includes vital protections for privacy and civil liberties - we are working to strengthen these provisions without weakening the important cyber security advancements it promises - and does not create any new federal spending, regulations or unfunded mandates.

Better enabling information sharing as outlined in Representatives Rogers' and Ruppersberger's bill is critical for addressing the cyber threat. This would help organizations execute with the alacrity shown by our cyber adversaries, as previously described. There are also other positive incentives that can help address some of the fundamental challenges ISP's, telecoms and other members of the communications eco-system have – challenges in hiring the right type of cyber security experts, regulatory disincentives, economic disincentives, and the immaturity of the insurance market, which has limited the growth of the kind of insurance programs needed for companies to insure against catastrophic losses:

· **Litigation/Legal Reform:** Imposing limitations on liability for damages as well as for non-economic losses would remove a serious obstacle to information security investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company's good faith investments in adequate information security. Eliminating that risk, at least for companies that meet high, "best practices" security standards, would encourage more security on a company-by-company basis. This approach can help create positive incentives for disclosure through liability relief for responsible organizations to improve the nation's overall cyber security posture.

· **Competitions, Scholarships, and Research and Development Funding:** Cyber security competitions and challenges, as well as scholarship and creativity to programs, can help identify and recruit talented individuals to the field to augment the future cyber security workforce. Similarly, research and development grants

foster innovation and advance basic and applied solutions. Recognizing this, several legislative proposals under consideration contain provisions designed to help industry meet the cyber security challenges of tomorrow and train the next generation of experts.

· **Tax Incentives:** Accelerated depreciation or refundable tax credits are being considered to encourage critical infrastructure industries to make additional investments in cyber security technologies, solutions, and human capital. The same approaches could be effectively applied to small businesses. Despite the current environment where balancing the budget is a critical priority, we cannot afford to be shortsighted. Cyber security-related tax incentives would prove to be a legitimate, long-term investment in security that would protect our national security and economic interests.

· **Insurance Reforms**: Many companies defer investments in improved security out of a concern that, even with improved security, they are not protected from liability for losses that occur. Similarly, insurance carriers are reluctant to create a vigorous marketplace for cyber-security insurance, thereby hindering investment. Government should give consideration to implementing reinsurance programs to help underwrite the development of cyber security insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gained experience with cyber security coverage.

Conclusion

ISPs play a foundational role in the global digital infrastructure. Industry and government should work together to help ensure that ISPs gain access to and use the most innovative technologies available to protect our networks and citizens from increasingly sophisticated and insidious cyber threats.

Collaboration and cooperation between the public and private sector are key to addressing cyber security in a holistic way. By combining government and industry's threat intelligence, communications networks of the future can create resiliency by rejecting harmful code in milliseconds just as our bodies reject viruses reflexively, without knowing the name of the particular disease they are fighting. Government can promote innovation of these tools with the use of positive incentives. The resulting advances will be critical to protecting our networks, communications, intellectual property, state secrets, critical infrastructure and national security. In the best American tradition of collaboration, the public and private sectors have made important strides already to address the cyber security challenge and enhance working relationships.

We acknowledge the tremendous legal and challenges currently faced by ISPs in sharing threat intelligence and encourage policy makers to enable ISPs to provide more of their threat picture to other public and private entities in exchange for the respective data from others. This can then be used to block the most harmful threats

from being routed to their intended destination. Unlike the biological or weather models, we can block the harm once we detect it.

ISPs are not solely responsible for cyber resiliency, and we encourage all system owners and operators to protect their network assets with technologies like those mentioned, which can detect and prevent harm even in computer hardware and memory. Many industries have a large role to play in protection, innovation, and the advancement of good science.

We believe our public and private collective goal for ISPs is to enable the ISPs to protect, learn, and innovate with us, based on a legal, policy, and business framework that promotes cyber resiliency, civil liberties, and good business around the world. We look forward to participating in the ongoing efforts to maintain the resilience of our communications networks, which are so vital to every facet of the nation's economy and overall prosperity.

Thank you for requesting McAfee's views on these important issues. I will be pleased to answer any questions.

Mr. WALDEN. Very impressive testimony. Thank you. Thanks for all the work you do to try to keep us secure.

We will now go into our question phase, and I wonder, Mr. Clinton, you talked about incentives and were fairly specific. Can you dive down a little deeper in terms of what that means in terms of more specifics on the incentives that would make a difference here?

Mr. CLINTON. Certainly, sir. Thank you. We are supportive of the approach that was articulated in the House Task Force report which suggests that a menu of incentives needs to be developed because different industries are responsive to different things. The defense industrial base may be attracted by a procurement incentive, the banking industry maybe by an insurance incentive, the utilities perhaps by getting rid some of the outdated regulation that is based in an analog form rather than digitalized. So you need to have a set of incentives.

On the other hand, you need to have some agreement as to what needs to be incentivized, and for that, what we have suggested and is in the multi-trade association paper that I spoke of before is that we need to have some independent entity which does not create the standards or practices but simply evaluates the standards and practices, an underwriters laboratory for cybersecurity, if you will, and then organizations would choose to elect a higher or lower level of adoption based on their business plan and their business plan would be improved because they would have access to lower liability costs, lower insurance, better chance to get a Federal contract, etc. So we are saying that we need a new system, not a government mandate system, but a system where there are government roles such as providing the incentives and there are independent roles, something like this underwriters laboratory, and then responsibility for the owners and operators.

Now, in those sectors of the economy where the economics is already built into a regulatory model, then you can use that regulatory model. You don't need a new regulatory model. You can use it. For example, if you are dealing with the utilities, they have generally a fairly detailed regulatory structure. The problem that they are having is that they get mandates at one level and the funding comes at another level so there is going to have to be a correlation done on the government side. But basically we think you need an independent set of entities indicating what needs to be incentivized. That can be done on a continuing basis. Government needs to provide the incentives and industry needs to implement them.

Mr. WALDEN. All right. Very helpful. Thank you.

Dr. Schneck, so when you and your sister were trading packets when you should have been sleeping, obviously, doing your homework, turn out the lights, that was when this threat was really computer to computer. Now we understand it to be bigger than that, broader than that and whole networks that can be taken down. So can you describe what those threats look like and what should happen there?

Ms. SCHNECK. Absolutely. We did that over a 1200-baud modem over a phone line.

Mr. WALDEN. I remember a 300-baud modem where you put the phone in the little coupler.

Ms. SCHNECK. Right. So the threat really looks at an instruction that executes off the site of memory, not the piece of memory in your computer that holds some word-processing program but it is where your computer grabs the next instruction, what do I do next. At the root of every exploit or attack, it is, I am controlling my will on your machine, whether I am telling your machine to send out a lot of traffic or adjust something that might change the settings on something that controls circuit relays on an industrial system. I am allowing—my will is being changed on your machine, I am executing on your machine. So as was pointed out earlier, you can buy these exploits on the Net. You can even unleash botnets together in a screen that looks like it came off of Quicken. It is a spreadsheet, and you can choose addresses to which to send it. You are simply relying on someone else's construction of a piece of code, and we see in McAfee labs 66,000 new variants of these pieces of code every day called malware that allow my will to be instructed on your machine.

So the idea is, well, it is twofold. One is to catch the IP addresses that are spreading it across the Internet and that goes to that threat position, sharing that global threat picture. I can't forecast the weather without the weather from all the different States or countries, and that comes from enabling the information sharing, but also the ability to detect an instruction that is doing something it shouldn't do. Resilience means I can run even if the enemy gets in so the enemy will get in. The biological analogy is the disease is in your body but it will never hurt you. So we have to let many instructions get in because they will and simply be resilient to that, and that is the ability to work at the operating system level instead of having to judge every instruction, are you good or bad, because we have shown that is not effective, just know what is good and don't let anything else run. That is known as application white listing in the community. And then down at the hardware level, understand what an instruction should be accessing or shouldn't and just block it, and we can do that.

Mr. WALDEN. I am glad you are on our side.

Ms. SCHNECK. Thank you.

Mr. WALDEN. Mr. Conner, you were talking about Zeus merging with SpyEye. Some of us wondered maybe that should have gone through like an FCC approval process for a merger and it would never have happened. All right. Now we will get serious.

I am going to turn to my friend and colleague from California, who brings so much to this discussion and debate, Ms. Eshoo, for 5 minutes for questions.

Ms. ESHOO. Well, I want to thank each one of you for your outstanding testimony. I think that this is one of the best panels that has been assembled on a given subject matter and it is highly instructive.

I can't help but feel that this is like trying to get socks on an octopus, though. I mean, it is massive. And I think that we all have a pretty good sense of what the threat is. I don't think that we have a clear picture of really what to do with it. There are so many agencies. There was a mention of a 1986 law that I want to hear more about. We have talked about public-private partnerships. We know that 95 percent of this is in the private sector, 5 percent in

the government. Where do we begin with this? What are the legal roadblocks as any of you see them right now that are holding us back to do what my next question would be, what is the new paradigm? And if we have very good pieces in place right now, what do we keep, what should we get rid of? And to Dr. Schneck, do you agree with this notion of Mr. Clinton's of an underwriters lab? That sounds very interesting to me.

So I don't know who wants to begin with what, maybe with legal roadblocks that you know of. I think it was Dr. Schneck, were you the one that mentioned the 1986 law? I am not familiar with that and what it is blocking.

Ms. SCHNECK. So I am not a lawyer.

Ms. ESHOO. Neither am I.

Ms. SCHNECK. But the overall premise and the reason I mentioned that is because the adversary has the ability to act on us very quickly because they have no roadblocks. We have the ultimate weapon, and that is, we own the infrastructure that works at the speed of light, and if we can put the instructions together and the intelligence together to work as your body does, it attacks a virus that comes in because it knows it doesn't belong there, it doesn't need to have a meeting to do so. We need the Internet to work the same way so the routers and the machines that route our traffic, they need to understand that something is bad, and to do that, we have to replace the chemical and biology with the intelligence from data and that means getting data from all sides of the equation that we control from the private sector. We have to be able to combine that with data in the government sector, not even in the classified realm. That would help, but this is all un-class. And then some of those laws actually prevent the ISPs from combining that data together. I don't have the answer legally on how to make that work while also preserving the civil liberties and privacy, which are crucial. But we have to find a way to put together at the indicator level this address, this location could hurt you and make that accessible to a router at several hundred gigabits per second.

Ms. ESHOO. Now, what you just described, would that fit in with Mr. Clinton's idea of an underwriters lab, or not?

Ms. SCHNECK. I think it is different.

Ms. ESHOO. It is different. OK. Did anyone ever tell you that you look like David Gergen? I was looking at you and I thought, I know he reminds me of someone.

Mr. CLINTON. Well, I am pretty flattered. I hear David is upset when the comparison is made.

I agree with Phyllis. I think that it is a—we are talking about kind of different things. First of all, with respect to the legal issues, after he got elected, President Obama appointed Melissa Hathaway to do a 60-day cyber review on the National Security Council staff and the largest portion of that is appendix A, which is a thick document going through all of the legal barriers that need to be reviewed, so that is a place to start.

Essentially what we have here is, we have a whole bunch of laws that were written for an analog world and we are now in a digital world. I mean, we have still laws on the books dealing with how you manage your videotapes. I haven't had a videotape in quite a

while. So there is a lot that can be done to work out that legal underbrush and modernize things. We have suggested some of those things are regulatory and could be offered as incentives, you know, to get away from some of these burdens. Some of them, for example, are duplicative auditing requirements. We are all for auditing but we should have one unified cybersecurity audit and you pass that audit and you don't have to do the rest of the audits but there are multiple State, local, Federal, different agencies that are involved in this, so organizations are spending a lot of their time and money doing redundant things. We should strip away a whole bunch of those sorts of things.

The last thing on where you start, I would strongly suggest that Congress start by cleaning up the Federal Government's roles and responsibilities. That is a much more limited system. You can make a lot of progress really quickly while we are continuing to work with a public-private partnership model that we currently have.

Ms. ESHOO. Thank you. I am out of time.

Mr. WALDEN. I will yield to the gentleman from Nebraska, Mr. Terry. Before I do so, it strikes me, we ought to get this appendix A and maybe have a task force of this subcommittee that really gets into the weeds and that more deeply, and we have got people who have great experience here.

Mr. TERRY. So where do we start, Mr. Clinton?

Mr. CLINTON. Well, as I said, I would start first of all at the Federal level. We need to straighten out roles and responsibilities of the Federal Government and between governments at the Federal, local and State levels. So, for example, I mentioned the problem that we have in the utility sector where we have mandates that exist at one level, the funding comes at another level, and what we have to do is realize that solving some of the cybersecurity problem is going to cost us some money. Unfortunately, when you have State public utility commissioners, they are resistant to increasing the rate base, and this is understandable, but we have to find some way to get a pass-through on some of these things.

So I think a good review and scrubbing of the governmental issues is one place to start. Simultaneously, we have a lot of activity already going through the public-private partnership that can use a number of these things. Mr. Rogers' bill is a good example. And then I think we need a really concentrated effort on working on these other incentive programs, exactly what do we need to do with the insurance industry to get them to be bigger players, exactly what——

Mr. TERRY. In what way?

Mr. CLINTON. Well, you know, private insurance is one of the most effective pro-social motivators we have. People drive better, they give up smoking, et cetera.

Mr. TERRY. So cyber insurance?

Mr. CLINTON. Cyber insurance, sure, so that if there is—the problem that we have in insurance, there is a couple of problems. One of the problems is, we don't have enough actuarial data because the data is being held.

Mr. TERRY. Doesn't Google have all of that?

Mr. CLINTON. Pardon me?

Mr. TERRY. I am sorry.

Mr. CLINTON. A lot of the insurance guys would like——

Mr. TERRY. You guys were good at humor. I tried it.

Mr. CLINTON. A lot of the insurance guys would like to share data but this runs into antitrust problems, OK, because to be sharing data for rates, but actually if we could get them to share that, perhaps in a public-private partnership, we would get a more realistic view of what the threat is. Right now they set everything at maximum, but if we share data, we could get a more realistic view of what the threat is. We think this would bring down insurance rates. When you bring down insurance rates, more people will buy the insurance. When more people are buying the insurance, more insurance companies will get in, and we get a virtuous cycle going on and we can use insurance to motivate better cybersecurity investment.

Mr. TERRY. All right. Mr. Dix, one question for you, and you can add on wherever you want, but you mentioned that, you know, for everyday users, small businesses, it is a just a matter of cyber hygiene, so I say, OK, you pull out your soap and you wash. What does that really mean and what can you do? What can we do as small business people or whatever?

Mr. DIX. So again, as I mentioned, I think we need a comprehensive and sustained national education and awareness campaign that tells the user constituencies how better to protect themselves from the infection in cyberspace. Leveraging the resources of the Federal Government such as the Small Business Administration, the Internal Revenue Service, the U.S. Postal Service, and other agencies that interact with citizens and businesses every day would be a place to help message that, creating and leveraging a model like we did with H1N1 where we have a sustained plan of public service announcements that drive people to a place where they can get information. It might even be nice if every Member of Congress had a link on their constituent Web page that directed folks to the National Cybersecurity Alliance or the Internet Security Alliance as a place to learn basic best practices, low-cost or no-cost things that they can do to protect themselves.

If I might add, another piece of the fundamental blocking and tackling is to ensure an operational capability that presents something like a National Weather Service or a CDC capability where we have a picture into what is going on in the networks at all times in steady states and in points of escalation. I raise that because many of us work together through the National Security Telecommunications Advisory Committee and delivered a report to the President in May of 2009 that recommended the creation of a joint coordination center, a joint public-private integrated 24/7 operational capability to improve detection, prevention and mitigation. We have got to get in front of this. Most of our time now is spent in response and recovery. Part of the problem we ran into, legal barriers. Once we got into trying to integrate, we developed a model in the private sector. Once we began to try and integrate that capability with the government, the lawyers told us they couldn't talk because they couldn't share this information. Hopefully Representative Rogers' bill will help break down some of those barriers, but we should have an operational capability that has a

picture as to what is going on in the network at all times and we have those kinds of data feeds available. Organizing them and having a National Weather Service or CDC type of capability is long overdue.

Mr. TERRY. Thank you.

Mr. WALDEN. The gentleman's time has expired.

I believe Mr. Waxman is next for 5 minutes for questions.

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

Dr. Schneck, and anybody else who wants to respond to this question, what special considerations do the growing use of smartphones and tablets present?

Ms. SCHNECK. Thank you. There are several. Smartphones and tablets are just small computers. They have the exact same vulnerabilities that all the other machines have that you are used to, and they have tens of thousands times of memory in them that the guidance systems do that took our first Apollo rockets to the moon. So when you think about the power that is in your hands, you now have the ability twofold. One is that it enables the enemy to, if it is not secured appropriately, it enables an adversary to use it as a platform to get into your enterprise network. In the interest of time, I am going to simplify this a lot, but people are wanting to use the home device at work, and what happens is, once the adversaries discover they can use that unprotected home device that happily houses Angry Birds and launch an attack into the enterprise network because companies are letting folks use the small devices.

So there are technologies to lock that down. We do a lot of that. We manage that worldwide. But you are looking at a massive explosion of small devices. The lady mentioned the cloud. These devices leverage the cloud because they don't have as much processing power as the big machine. So most of your processing is done in the cloud. You have to pay extra attention to the security on that motion data at rest and shared resources where your data are when they are not on the phone. Your personal information most likely is all over that phone, pictures of your friends and family, locations. If you lose it, you want to make sure you have a remote capability to destroy that. It is a wonderful device, but it has access to, again, all the critical infrastructure. If you are working on one and it is talking to your network, it has access now to your personal information.

So I think it brings a wonderful new—I spoke about this at the consumer electronics show. It brings a wonderful new sense of fun to computing and it also brings new dangers that we need, to quote my colleagues here, to get out in front of before this is yet another massive vector because mobility is multiplying.

Mr. LEWIS. Just real quickly, every once in a while I talk to hackers just to see what they are up to, and recently one of them told me that the price for a toolkit to hack an iPhone is about $200,000 on the black market, and he said for other phones it is only $10,000. So, you know, I don't know. What this is going to do, though, it is going to force us to pay more attention to the service providers, to the big telecos, to the ISPs to the cable companies. Responsibility is going to shift away from the edge, away from the consumer to the service provider.

You don't patch your cell phone. You know, you don't program it. You depend on its computing becoming a service, and that will change the contours of security and change the requirements for regulation.

Mr. CONNER. With all due respect, I disagree with that. If you look at Metcalfe's law and if you look at just what happened with Apple and AT&T, the value has shifted. It shifted from the carriers to the endpoints, and this is about identity, and I will give you a good example. The threat I talked about going out of band or using a mobile network and a device is a surefire way to stop that kind of transaction today, and it is safe and it is protected. It uses digital signature through a wireless carrier network and on a mobile device with digital signature which is probably why to try to hack the device costs a heck of a lot more on an iPhone or iPad than a normal phone. And if you use that, the probability on that attack factor, you don't break it.

So I think there are good pieces and I think my personal experience, the minute you think you are going to stop all this in the network, the ID and IP address is no longer the identity. The number one thing people fake is who you are, what you are, and the application of who are you, and that is the hardest thing to combat in terms of good guys versus bad guys. The threat I showed you is not the identity of the person that is doing it. He has faked your identity, and no perimeter technology, no network can deal with that until they deal with the endpoint itself.

Mr. LEWIS. I don't think we are disagreeing, though. I think that you are going to see that the authentication technologies you are talking about will depend ultimately on the service provider.

Mr. WAXMAN. Well, let me ask one question, and I know I don't have much time, but many of you mentioned in your testimony how communications networks are central to most other critical infrastructure sectors. How does this then relate to the importance of this committee in addressing cybersecurity of communications networks? Anybody want to respond to that?

Mr. LEWIS. Well, I think that in the opening remarks, a few of you mentioned some of the things that are going on at NTIA and FCC that could reduce risk, right, and one of the examples we have heard about is of course this measure to get the Internet service providers to adopt a voluntary code of conduct for dealing with malware. It is a good thing to do. It is sort of basic-level stuff. The FCC has an effort to promote the use of DNS security, DNSSEC, and this is—not to get too complicated, but this is a growing vulnerability. It is relatively easy to fix. Other countries have moved faster than the United States. It is something that we can probably do on a collaborative basis.

The third thing to look at is some of the responsibilities for other activities, other protocols. This is a place where you don't want the government creating technology, right. It is not for this kind of level of technology. But you do want it maybe coordinating a response, and so when you look at FCC, when you look at NTIA, the DNSSEC, the ISP efforts, some of the other measures, Commerce is doing similar things, this is where you can play a big role.

Mr. WAXMAN. Thank you, Mr. Chairman.

Mr. WALDEN. With the committee's indulgence, we were all going to ask you about the Australia model, and then we all forgot. Without objection, would you mind addressing the Australia model?

Mr. LEWIS. Well, Phyllis talked about this as well. Your ISP probably has a pretty good idea of what is going on on your computer at home, right, and right now they don't really do much about it, and I think Bob talked about this as well. You know, there is basic hygiene things that most people don't do. Your ISP has fairly good knowledge when you are running malware, when you are part of a botnet, not perfect knowledge but good knowledge. What actions can they take to stop that? And in Australia, Australia is not the only country that does this anymore, at one point they thought the attorney general will come in and tell the ISPs what to do, because the ISPs were not doing anything. This was a failure of incentives, right. And there was a tussle, a political tussle. At the end of the day, the ISPs—and Australia is a little easier because it is a smaller country. They said how about if we come up with a voluntary code of conduct that will let us deal with the malware threat, and with a little guidance and help and involvement from the attorney general and the Australian federal police, which is roughly equivalent to some of our Federal agencies, they came up with a pretty good system that works pretty well.

This will not deal with the advanced threat but it will deal with—you know, quick, name a country in the world that is the biggest supplier of botnets used in cyber crime. It is the United States, and it is not because we are cyber criminals, it is because we are incompetent in our defenses. The Australian model changes that. We are number one, hey, great.

There are some issues, and I will just do them quickly. Other countries that do this—Germany. Germans have a lighter approach. What happens in Germany is, you get a little popup on your screen that says basically we notice you are infected, call this number if you want help. Australians and some of the other countries that do this say click here and we will clean your computer for you. A few other places that don't go public, they just intervene without your knowledge. You have a privacy issue. You have to be careful about that. One of the things that comes up over and over again is, Should we isolate infected computers? Should we cut infected users off from the Internet. Some companies are beginning to do this. You are putting such a burden on me that I am just going to cut you off. A big issue. If you look at the places where we have data, there is an amazing drop in the rate of infection. So this works, and it would be useful if we followed the Australians, the Germans, the Japanese, the Turks, any number of countries.

Mr. CONNER. I will give you two other points on Australia that are, I think, relevant to this group. Australia is also looking at their energy grid, and granted, their energy grid is a little different architecture than the United States, more like Ireland and others, but in the process that we are working with them, they are starting with the infrastructure part and the actual production side, the energy creation, one, to lock down the authentication of the systems within the creation of the power and starting there, and then going to the export of that power through the grid as it extends through the different carriers all the way to the endpoint in terms

of that. We are involved with other companies here in the United States helping them do that.

The other piece is, as they look at health care, they think that is a critical area in terms of being able to have health care cards, a novel idea when you get to privacy concerns here, but as I say, you can't have privacy without security and policy.

Mr. WALDEN. Thank you, and thanks for the indulgence of the committee. I am going to go to—oh, Dr. Schneck. I am sorry. Go ahead.

Ms. SCHNECK. One point, if that is OK.

Mr. WALDEN. Yes, sure.

Ms. SCHNECK. So I think that the example in Australia is a beautiful example of this need for information sharing. I would challenge the wording a little bit from Dr. Lewis, and I don't think he meant it this way, but the ISPs don't know what is going on in your computer. They are not watching your banking. They are not watching you work. They see because they own that block of addresses. They see the behavior from that block of addresses as a footprint as it tries to send traffic, which the ISPs are able to track to protect you from malware. They see that footprint, just like McAfee sees it, reflect on things they own, and from that they can see where traffic has come in, for example, a ridiculously large volume in a short period of time from a certain set of machines and they can look at those machines and say these are infected with certain code, and they can then, in the Australian model, let you know, and so the question becomes, how do they let you know. I think it is a great example of the use of that intelligence picture. It shows how with Representative Rogers' work, we could actually get a larger intelligence picture. That is what makes for the humans that the pretty weather map picture that Mr. Dix recommends. But also, you have the ability now to look at who is infected where and start looking at these incentives. How do we incentivize the general public to do this hygiene? Most people with a computer don't know what it does all night when they are sleeping. If they knew, they would clean it up. It is not that hard. So I think this is a really neat exercise on the information sharing and the incentives.

Mr. WALDEN. I appreciate that, and I appreciate the committee's indulgence in just trying to get some more information out there.

Mr. Rogers, thank you.

Mr. ROGERS. Thank you very much. I know we are short on time.

Mr. Conner, are you familiar with the company DigiNotar or what used to be the company DigiNotar?

Mr. CONNER. Very much so.

Mr. ROGERS. And signatures and attribution is very, very difficult, although I think we are getting better. It is pretty difficult. Can you briefly—I think it would be good for the committee to hear the story of DigiNotar and how a viable company went away in about a month after being hacked and what it does, quickly, and what happened and why this is important to move forward.

Mr. CONNER. So if you look at the Internet when it was created, the little yellow lock, everyone sees the little yellow lock on their browser and on their PC and they think they are safe. Very few people know what that little yellow lock means, and what it is sup-

posed to mean is the communication path is secure between you and the Web site that you are communicating with and who is on each end of that. The problem is in the SSL world, which is kind of the security level of that, the identity on each side of that may or may not be who it is reported to be. We co-chaired along with Verisign a new standard on that extended validation because if you go to your Super Bowl last week, you will see people advertising, hosting and selling that little yellow lock for $19 for your business Web site. The only problem is, the verification of who on the end of that is, is pretty lax. And they just look at the server and go well, that must be you.

So the issue was, this one company that provides the little yellow lock, in this case, predominantly in the Netherlands, was breached, and they were breached from Iran just as many other security vendors have been breached. We get a target every day from country states, our little 350-person company with no help to the U.S. government, thank you very much, to defend that. Well, this little company got attacked just like Comodo did, just like others did, and they breached that little yellow lock that said who they were and they began to take down the government security because that government used the little yellow lock for all its online capabilities, and the people in Iran, guess what, used that little yellow lock to say they were Google and other people. So anyone in Iran that was Googling content in that country was able to give up to the Iranian government whatever they were looking at, whatever they were doing, and one government was basically shut down for at least 60 days, and unfortunately, to those of us in the security world, we found out about it through the browser forum and actually Entrust was a partner to that group, and it ended our relationship with them prior to that, and even we weren't notified. So that talks about to your question of the legal framework of what is going on here and the disclosure requirements.

Mr. ROGERS. Thank you. And I just think that was a great example of a nation-state using its intelligence services to co-opt something like that. And by the way, DigiNotar is no longer a company, so if you want——

Mr. CONNER. Yes, it is out of business.

Mr. ROGERS [continuing]. To talk about the cost, there is a hack that took this company and is now out of business, so——

Mr. CONNER. Well, be careful. It was a subsidiary of a public business that still exists that acts like it didn't happen.

Mr. ROGERS. But the contracts that it has in the Netherlands no longer exist?

Mr. CONNER. No, that is correct.

Mr. ROGERS. OK.

Mr. CONNER. That is exactly correct.

Mr. ROGERS. It is an American company that actually owned it?

Mr. CONNER. That is right. And I think the point that you are on, Congressman, is an important one. There are ways—we have been attempted to be hacked by the same group. We have watched them try that over the last 12 months. Two of the people that own the yellow locks in the United States and abroad have been taken down relative to Iran being able to break in and impersonate those pieces. So it is happening every day.

Mr. ROGERS. I thought it was important for the committee to hear that particular case because it shows how sophisticated and how dangerous it can be if somebody has a nefarious purpose other than criminal. Criminal is bad enough. This was other than criminal. And I see my time is almost up so I am going to ask two questions and close up.

Mr. Lewis, I would like you to talk about, we have been through a long time. It has been very difficult to get to a place where we have a very narrow focus on how to move to the next step. Just talk about the challenges of why we think it has been difficult to even get a very narrow change in the law.

And lastly, Dr. Schneck and maybe Mr. Dix can talk about this, you talked about hardware. There is much concern about hardware entering our system that may be malicious and very difficult for us to understand exactly what that hardware is doing in our systems, and I am hoping you can talk about that and what we might be able to do from a regulatory and/or cautionary position on behalf of the United States Government to make sure that those type of hardware systems don't enter our system and some of our hardware systems are not exposed when they leave this country to manipulation by foreign nation-states.

Mr. LEWIS. Thank you, because those are hard questions. They are great questions but I am glad Phyllis got one of them. So, you know, the neutral answer is to say when you look at a new technology, it usually takes the United States somewhere between 20 and 50 years to figure out to get it in order. So you look at airplanes, steamboats, railroads, electricity, cars. We are in year 18 for the Internet. So we are not doing too bad, I guess. I mean, we have a couple years to sort this out.

A little more pointed answer: We have so many old ideas. They have not gone away. If it was in PDD–63, which was the Clinton administration policy, and we are still trying it, it doesn't work. Give it up. And the second thing is, as you have heard, we have old laws that are real obstacles. You of course are trying to fix this but if it is the Electronic Communication Privacy Act designed for dial telephones, you have serious issues here. You have business issues, you have privacy issues. So it is a hard problem and it will take time to work out, but the prevalence of the old thinking and the difficult legal environment we have has really slowed us down and put us at risk.

Mr. ROGERS. Mr. Dix or Dr. Schneck?

Mr. DIX. First of all, I would like the record to reflect that Mr. Lewis and I agree on that last point. Thank you. First of all, let me just touch on the hardware issue because the whole supply chain risk management issue, you know, it is interesting to me, the last count, there is 155 different supply chain risk management initiatives in the government today. We need to coordinate those issues. And quite frankly, organizations like ours, we invest heavily in what we call our brand integrity program because our reputation is how we grow our business. So we invest from concept to delivery in our products, in our hardware and software products.

To make this short, one of the things that I think that this body could help with, as we sit here today and we deal with this supply chain risk management problem, the Federal Government still con-

tinues to buy from untrusted sources. There is a cultural cost to government of cost and schedule across the departments and agencies where in order to save 5 cents on a widget, we are buying from low cost, low bid. As a result of that, we end up in the gray market and then we wonder why we have counterfeit or malicious products in our government supply chain. We should be buying from trusted sources. If there is some reason why we are not going to buy from trusted sources, there should be a justification, it should be public, and the liability from that should accrue to whoever the acquirer is.

Mr. ROGERS. Dr. Schneck, can you just comment on that as well?

Ms. SCHNECK. I do agree. I will also add that we look at supply chain again as an issue of your product integrity. We do rigorous testing, both the manufacturing and acquisition. We would also believe in leveraging some of the existing standards to really focus on a product integrity issue, because what you want to know is, did that widget that you bought, is it exactly what you think you bought. That is the heart of the issue. So it is rigorous testing and expanding some of the existing standards.

Mr. ROGERS. Just to clarify for the record, Mr. Chairman, so we are at risk if we integrate into the U.S. system non-trusted sources of product? I want to make sure I am clear on that.

Mr. DIX. I certainly think it increases the risk.

Mr. ROGERS. Thank you.

Mr. LEWIS. I used to do the supply chain stuff when I was in the government sort of on both sides of the table, and a couple points on that. First, right now it so easy to hack, you know, that you have to assume that our Chinese and Russian friends are taking the low-cost approach to espionage. Why should they not do it? The second one is, it is very hard to push this out to a global supply chain. We are not going to be able to get out of that. So this is an exceptionally difficult issue that will probably force us to think about how we are going to work with foreign suppliers. And there is not really a choice here. So what I do think will happen—I will just say this real quick—right now hacking is so easy, why bother. If we ever manage to improve our defenses, they will switch to supply chain.

Mr. WALDEN. I appreciate that. Here is the problem. I am 5 minutes over his time and I think members are——

Mr. ROGERS. But this is a Clinton we can all agree with right here.

Mr. WALDEN. The gentleman's time has long ago expired, and I appreciate the patience of the committee members who haven't had a chance to ask a question yet, so we will try to get back on schedule. Mr. Doyle.

Mr. DOYLE. Thank you, Mr. Chairman. Thank you for putting this hearing together, and to the panelists, your testimony and your answers to the questions have been very informative.

I want to follow up on a line of questioning that Mr. Waxman had to Dr. Schneck. Dr. Schneck, I know in your testimony, McAfee labs predicts an increase in attacks on smartphones and mobile devices in the future, and it is my understanding, your company had partnered with a research facility at Carnegie Mellon University sci lab, which is in Pittsburgh, the district I represent, about how

businesses and employees handle mobile device security, and apparently this study showed that most of lost and stolen mobile devices create some of the biggest concern for businesses. About 40 percent of the organizations surveyed have had lost or stolen devices and half of those devices contained business-critical data. Further, about 50 percent of mobile users that were studied, we found out they store their passwords and their PIN numbers and credit card information on their mobile devices, which I am completely guilty of. I am going to erase them as soon as this hearing is over.

It seems to me that one way to tackle this is to make sure that the devices that employees are using are secure in the first place so that if an employee uses them, that the data remains secure or you could remove that data from a remote source, and to follow up with what Mr. Waxman asked you, to your knowledge, could you elaborate on what is being done by device manufacturers and app developers to secure their products for commercial use?

Ms. SCHNECK. So we look at protecting them once they are received so from what we have worked with, there are a couple of vectors on what they are doing before delivery. You know, one is—I will take the application side first. When people download an application, they rarely think about is this application secure. One of the biggest dangers we see is not did I catch a virus, it is did I go and purposely download something with a big smiley face on it and a great app that did something neat for me, but what it is actually is, it is a pretty picture and delivery of malcode. One of those instructions will get to be a platform to enter your network corporate or to start shipping back your personal information for sale in the Russian underground. So that is one risk. And the app developers, so some companies are very careful in the app markets and only approved or back to the trusted source point, the only approved apps are there for sale. Other companies are more open about it and it is up to the user to be very careful about what you download.

Mr. DOYLE. Mr. Conner, do you have some thoughts on that?

Mr. CONNER. Yes. We work with all of them, so from the Android operating system to iOS to the Microsoft, the first thing we are working with each of them on is, how do you identify the device itself securely and authenticate that back to your company, because if you don't know it is connected to your company, you have got your first issue and kind of the consumerization and the enterprise.

The second theme becomes, how do you then work with the applications that go into that phone, and each one of those ecosystems do that differently. Some have sandboxing where they then can use our security or others to make sure they know who is coming in to put that there. They all three have very different testing mechanisms to test those apps in terms of that sandbox and how they communicate that back and forth. And then the third thing we are working with each of them on is how you secure email and content and communication, whether it is mobile, no different than we did with laptops and desktops before.

Mr. DOYLE. Mr. Dix?

Mr. DIX. Yes, and good old U.S.-based innovation has delivered today. Available in the market today, a capability to lock, locate and wipe those devices on demand.

Mr. LEWIS. We are getting close to maybe having a solution to authentication. It has been the holy grail for about 20 years.

Just a quick story to help put this in perspective. There used to be just one government-approved private company in North Korea. Do you know what they made? They made mobile phone apps. I see a pattern.

Mr. DOYLE. And just another general question for the panel. Do you think the FCC has any role to increase mobile device security, and what should that be? Mr. Conner?

Mr. CONNER. Absolutely. In fact, you look at the FCC, the critical infrastructure there. I mean, I spent 10 years at AT&T and another 10 putting electronics and systems into those type of companies. It starts with that. I mean, I said you can look at the mobile networks as either good or bad. It can stop the crime I talked about today if used correctly with technology that cannot be broken today. So I think that if you think of one governing body trying to own each of these pieces, it is folly. I think DOE needs to work with the public partnership and private partnership for its domain. I think Commerce and Treasury needs to work it, and I think FCC needs to own that infrastructure around that ecosystem because to think that the attack vectors that the bad guys are taking against us are one size fits all is just ludicrous.

Mr. DOYLE. Very good. Mr. Chairman, thank you.

Mr. WALDEN. Thank you, Mr. Doyle.

We will now go, I think Mr. Gingrey is next in order.

Mr. GINGREY. Mr. Chairman, thank you.

This question is for the entire panel. Maybe we will start with Mr. Conner. Some have argued that before we enter the cybersecurity debate, we should heed the Hippocratic oath and make sure that in the first place we do no harm. If there were one caution that you could offer us before legislating, what would that be? Mr. Conner, why don't we start with you?

Mr. CONNER. Well, I think the way I would start as a government is the bully pulpit, frankly. I spend a lot of my personal time with this team and others, spend a lot of time educating, and I think quality is a great example that this government got right. They didn't need equality. They just got on the bully pulpit and said quality is important. And when I think of security, the lexicon was not here. It still isn't here the way it was. If someone started quality, saying I am going to get to six sigma, they wouldn't know what it meant when quality started before the book. You heard cost equality. I hear cost of security. We are focused on what cost. Are you focused on the total cost of security or just the cost to implement something? So I would start with education and your bully pulpit.

The second thing I would start on is the inability of businesses to talk to governments or to themselves because of antitrust and the patchwork legislation in the States. I am tired of it being it a one-way communication street to intelligence and nothing in return, and I understand they legally can't do it, but as the company that is tasked with protecting our government and governments

and enterprises and citizens, it is pretty folly to me. I can only give you information; you cannot give me any.

Mr. GINGREY. Mr. Conner, thank you.

We will go to Mr. Dix and move rapidly.

Mr. DIX. Thank you very much. Two quick things. One is, continue to inspire and drive an environment that supports innovation and investment, and secondly, be cognizant of the fact that the bad guys move fast. We need to have speed, nimbleness and agility in our ability to respond. Attempting to comply with a compliance model that takes a long time to build and implement slows us down and imposes impediments to our ability to have speed, nimbleness and agility.

Mr. LEWIS. In 2007, we had an intelligence disaster——

Mr. WALDEN. I don't believe your microphone is on.

Mr. LEWIS. In 2007, we had an intelligence disaster in this country. The details are still largely classified. In 2008, DOD's Supernet was hacked. We were unable to get the opponent off for about a week. In 2010, we saw Google and about 80 other companies get whacked, lose intellectual property. Most of them have not reported it but this will show up in Chinese products in about 5 years. Last year we saw Stuxnet, which was the ability to destroy physical infrastructure using cyber attack, and we have a list at CSIS of major cyber events, mainly because I got tired of people asking me when we would have a cyber Pearl Harbor. The list is up to 90.

So I think what we need now is, we need to stop saying do no harm. We need to move out. We need to do a coordinated defense.

Mr. GINGREY. Dr. Lewis, so you think we definitely need legislation?

Mr. LEWIS. I do, and I think there are things—one thing that we can say now that we couldn't have said 5 years ago, we now have a pretty good idea of how to do this between the experts up here, some of the other places. There are agencies that have done a particularly good job. We now have a good idea of how to reduce risk and we need to implement that.

Mr. GINGREY. Mr. Clinton?

Mr. CLINTON. I agree that we do need legislation. The question is, what is the legislation that we need. I do subscribe to the "do no harm" theory. I think the one thing that I would tell the committee is to understand that this is not a technology issue. It is an enterprise-wide risk management issue. The problem we have is that in the cybersecurity world, all the incentives favor the bad guys. Attacks are cheap. They are easy. They are really profitable. It is a terrific business model. Defense is hard. We are following the attackers around. It is really hard to show return on investment to what you prevent, and criminal prosecution is virtually nonexistent. So I would go back to the last thing I said before I finished my oral statement: Understand that you are dealing with the invention of gunpowder. This is an entirely different thing. You can't just take 20th century models and plug it in here because you can pass legislation that will do harm, that will take away needed resources from where they need to be. We need a creative 21st century approach, and a lot of what we are seeing in the public policy world is not that.

Mr. GINGREY. Mr. Clinton, thank you.

In the last 12 seconds, last but not least, Dr. Schneck.

Ms. SCHNECK. Let us take this is an opportunity, unleash the power of the private sector. We built this thing. We didn't build it with security. Now we understand this adversary. Let us take the information we have, the data we have, the ISPs see all the mobile phone activity. They can see that. They can protect that. Incentivize us so that we can still eat when we get done doing it but let us make sure that we build business models around building security in from the hardware up, and I think you will see this world change in a few worlds.

Mr. GINGREY. I thank the panel for their excellent responses, and Mr. Chairman, I yield back.

Mr. WALDEN. Thank you, Dr. Gingrey.

Ms. Eshoo and I were talking about, we are going to lock the doors and not let you out until you give us all the ideas that we need to do here, and we will let you out today. But seriously, in terms of helping us understand how to get this right. You have a lot of them but in your testimony but if you could help us drill down very specifically, at least within the jurisdiction we have, we would really appreciate very specific suggestions back.

We are going to go now to Ms. Matsui from California. Thank you for participating.

Ms. MATSUI. Thank you, Mr. Chairman, and I have to say, this is probably the most interesting and scary testimony I have ever heard. But I think that quite frankly, our country doesn't realize what risk we have, and I think the things we hear about over the news are things—talk about hacking but they are at a level, a personal level that people understand. This is far beyond that. It really affects every sector of our economy, our country, the way we live. So I truly believe that this education process is going to be very, very important. And I also believe that people like you have to step up to talk about it in ways that the public could understand. Cybersecurity, everybody sort of understands it but doesn't understand it. So I think with every advance in technology, we open ourselves up, and our daily lives can be impacted so much.

I wanted to follow up a little bit more on the cloud-based services. Businesses and governments are now going into the cloud, and what are the unique challenges facing the cloud with respect to cybersecurity and are we prepared, are we thinking ahead, knowing what we know now about how we address these challenges, and why don't we just start over here with Mr. Conner?

Mr. CONNER. It is something that is getting a lot of attention from everybody, and I think a lot of people are running before they thought it through. I think it is very application and business sensitive, depending what you put in the cloud. Some stuff you put in the cloud, it is user name and password sensitive, that is fine, but if you are putting valuable financial information and intellectual property in the cloud, you have two issues. The security within the cloud is not what the security was within a mainframe data center today, and how do you authenticate to the cloud is still a matter of how you choose to implement that, and I think that is very naive.

Ms. MATSUI. So are we still at a place though where we could start looking at that and incorporate, you know, how we integrate

some of these things into some of the information-sharing activities. We are still OK right now, but right now you talk about the cloud as a very sexy thing so people are now jumping to it.

I was curious also, Dr. Lewis, that you mentioned that government should find ways to incentivize companies, and Dr. Schneck was talking about the same thing. What types of incentives would be the most effective, in your opinion? And I would also like to hear from Dr. Schneck too.

Mr. LEWIS. There are basically four kinds of incentives. There is regulation, and we are going to need some of that, not too much, and it varies from sector to sector. There are tax breaks. I mentioned this to the Republican task force on cybersecurity. They thought this was not the best year to go after tax breaks. There are subsidies, right, and we might need subsidies for research and development, perhaps some other things. Finally, there is a coordinating effect, right? Someone has to lead, and you can find this—maybe a good story from the Australian example. If you pull industry together and point them in the right direction, they will come up with some really good stuff and we can find some examples in the Defense Department where that has worked pretty well. So regulation, tax breaks, subsidies, and that might include building something into the rate structure for some critical infrastructure, and then coordination.

Ms. MATSUI. Dr. Schneck, do you agree?

Ms. SCHNECK. Not entirely. I think regulation draws a box around the technologies that you are forced to adapt. It puts all your money there. It takes it away from science innovation, and even worse, it shows the bad guy what we are not protecting. But I do favor the rest. I favor tax incentives. You know, we believe in insurance reform. Anything that allows a company to be creative, invest upfront in cybersecurity, because the upfront investment is a lot easier and a lot more fun than the cleanup, and it is a lot cheaper. I testified earlier a couple months ago about small businesses and incentives being needed when—we don't realize the small to medium businesses make up, you know, 99 percent in some cases in our business fabric, and if you think about where some of the newest technologies come from, not just cyber but maybe our jet engine comes out of a startup of a couple really bright guys out of college, they are not going to invest a whole lot in cybersecurity necessarily when they get that huge SBIR grant, but if built into that grant was some positive incentive or some extra money saying you will get this money from the government only if you promise to secure it, and we could be doing that for all levels of companies.

Ms. MATSUI. So government does have that type of role, though, and I think the part that I am looking at is, who convenes all this way? How do you do this so you all work together? Because I think you are absolutely right, the business sector can work together and have the solutions but how do we get to the next point?

Mr. CONNER. Well, I think the first thing you have got to do is relieve the legal obligation when we sit with CEOs. In my first public-private, all the CEOs agreed until they went and talked to their legal counsel, and guess what? Then it went completely dead because no one wants to go public. For one, you have got an anti-

trust issue of sharing, and second is, the minute you go public, you create a standard to be sued criminally as well as civilly, and that is the reality as a government person doesn't understand, but if you are a CEO, class actions mean something and suits mean something, and the minute I say something, I now put a different standard to me to be held to.

Ms. MATSUI. Well, thank you very much. I see my time has run out. This is very fascinating.

Mr. WALDEN. Thank you.

We now go to Mr. Latta from Ohio. We look forward to your comments as well.

Mr. LATTA. Well, thank you, Mr. Chairman. I appreciate it. And I thank the panel for being here. For someone who did serve on the cybersecurity task force, I can tell you, it is like you go home, go to your office, it is like, do I really want to turn that thing on now or not.

And if I can go back first, Mr. Conner, you know, talking about the yellow lock that you engaged with Mr. Rogers in a discussion about. You know, a lot of times they tell you if the https comes up, you are safe. Are you going to tell me that is not true now?

Mr. CONNER. The only thing I would tell you is, unless that chrome goes green, I wouldn't assume that you are safe.

Mr. LATTA. OK. Because the reason I ask that, you know, we have to get this message out to our constituents and the American people, and I know that a lot of folks see that little yellow lock come up and say I am fine. I hate to say that my daughters were on some social networking and we had a problem for about four days before somebody could spend—I don't want to say how much money it took to get the thing fixed before we could get back on the computer. But, you know, I am really very cognizant of the fact now of watching for that https to come up, because again, it also goes to the whole point of, you know, again, let us say you do online banking or people do certain things, we need to be able to communicate that, so that is one thing.

If I could ask Mr. Dix and Dr. Schneck this question. You both mentioned in your testimony the idea of creating trusted relationships online either through authenticated emails or through white lists. Could you elaborate on these ideas and explain how they differ from the previous cybersecurity measures like spam filters and blacklisting?

Mr. DIX. Ladies first.

Ms. SCHNECK. So our focus on trusted relationships are in the macro and a little bigger. I would say that we all need to work together, and we do. Organizations such as Bob mentioned, organizations such as the NCFT and the InfraGard show that government and private work together. I think we are dealing online today with a world much different than spam filter. I used to help build a spam appliance many companies ago, and what we looked at then was only the email vector. Now you have the web vector, the firewall vector, the mobile vector. Again, the enemy is faster. So when you start looking at trusted relationships online, we had at least 30 different parameters we looked at just at email. It wasn't just, "Did I trust the sender?" It was all kinds of things and indicators in that note. And now you multiply that. So you have, from our

perspective in protecting against cybersecurity threats at all the different vectors, we have over 1,000 different parameters of trust that we look at, and it is not just an established relationship. It is what has your behavior been lately as in the last two milliseconds and the last 15 years.

Mr. DIX. Continuing to advance the development and implementation of the national strategy for trusted identifies in cyberspace is a step in the right direction, and that is an example where industry and government working with NIST have come together to deal with this issue of identity. Every one of my colleagues here has mentioned the issue of identity as being a root issue in this entire trust discussion that we are having here today. So there is an effort underway. It is collaborative. It is producing results and moving to implementation for the in stick would be a step in the right direction.

Mr. LATTA. Mr. Conner?

Mr. CONNER. Just the last comment on that is, the irony of this is, you think of who are the most trusted identifiers we use. They are usually government issued. And I think this is one area our government needs to get out of the U.S. think and into the rest-of-the-world think.

Mr. LATTA. Let me kind of go on with this, because, you know, again, when you are looking at, you know, people trusting what they are doing on the Internet and banking, I don't care what it is, but when we were talking about trust, this is another discussion that was held a little bit earlier, you know, talking about not buying from the low cost, low bid and you need to buy from that trusted source, but how do you know? How do you know even if you buy from somebody that is trusted that that stuff is still good without going—I mean, how do you go through unless you are testing? Are you testing constantly? I will throw that out to all of you.

Mr. DIX. So since I brought that up, I will take that first, with your permission, sir. So each of us that are manufacturers has a network of authorized resellers and distributors that we utilize in the distribution of our products into the marketplace. That is a place to start from, understanding who those authorized providers are. There is also a great deal of work that is going on right now through the Trusted Technology Forum and the Open Group to be able to create a certification and accreditation process for suppliers, working collaboratively with the government again in a standards-based approach to being able to address this issue. So there is some good work that is going on right now, but the fundamental piece of it in my mind is cultural. We are still evaluating people and departments and agencies on their ability to meet cost and schedule. That drives a certain behavior because it doesn't have security as a paramount foundation of that conduct.

Mr. LATTA. Mr. Chairman, I see my time is expired and I yield back.

Mr. WALDEN. Thank you very much.

Dr. Christensen, you are now recognized for questions.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman, and thank you to all of the panelists.

This is a general question. The FCC's Communication Security, Reliability and Interoperability Council has been formulating rec-

ommendations for best practices to ensure optimal security and reliability of communication systems, so how do you see this process contributing to improvements in cybersecurity, or said another way, what is FCC's role in the coordinated defense that we heard about?

Mr. LEWIS. I am really glad you said that because I have been sitting here trying to remember what CSRIC stood for. I had gotten all but two of the letters.

We have all said, when you talk about cloud, when you talk about mobile, that we are moving to a world where the role of the service providers is going to be more important, and that is where FCC and NTIA are the lead agencies right now. There are others of course that are involved but FCC originally looked at this issue and they were afraid that if they took too active a role, as I understand it, they might be seen as trying to regulate the Internet, and they wanted to avoid that. So instead, they have taken on an approach that works more on coordination with private sector experts, with developing venues for these private sector experts to get together and encouraging them to come up with a voluntary approach, and one of the things I had said to FCC staff a while ago is, try the voluntary approach, and if it works, great. If it doesn't work, then we have to think about more mandatory measures. So far it looks like it is working, though. So I understand they have some measures they might roll out in the next few months. Commerce has some other things they are doing. This is where the service providers and their regulators will be one of the key elements of cybersecurity in the future.

Mrs. CHRISTENSEN. Anyone else?

Mr. DIX. So they are in a position to serve in a key role in this education and awareness campaign that we talked about and coordinating that at the national and in a sustained manner to help deliver messages to constituent stakeholders whether they are home users all the way up to large enterprises, working with the carriers and the content providers to be able to help deliver that message. So I think there is a key role in that part of it in showing leadership around how we advise people how to protect themselves.

Mrs. CHRISTENSEN. Ms. Schneck?

Ms. SCHNECK. Just one point in addition, having worked with them a bit over the past few months, they are setting a great example. Their house is in order from a cybersecurity perspective. They have some new leadership and they are really looking—they are reaching out to the private sector saying what are the best practices. They are reaching out, from what they tell us, to other CIOs and the government. So when you talk about the need to get the government's house in order, I think that is an exemplary piece. And in addition, they have a group of people really looking at these policies and really looking at these issues. We have never seen that before. So I think this is a good time for them to not only build on the awareness they launched, I believe it was last spring with the SBA to the hygiene program point, but then jump on that for the larger enterprises also as an example.

Mrs. CHRISTENSEN. Well, Mr. Conner, and this is probably what you are referring to at the SBA, but your testimony notes that according to the FCC, three out of every four small and mid-sized

businesses report having been affected by cyber attacks. So what is the role of the FCC in preventing the attacks or aiding the small business community?

Mr. CONNER. Well, I think increasingly the networks underpin all those attacks so you have got the ISPs, you've got the carriers themselves and you got the devices attaching to it. I think one of the areas that we must remember is, is it not always outside where those attack vectors come from, and just like organized crime found its way inside organizations, I think increasingly we are going to have to look at that as an attack vector, and that should be something that the FCC takes into consideration as they look at how to deal with it in addition to the ISP filtering and the other pieces they use.

But one thing I would caution, I hear a lot of rhetoric around building separate networks, and having lived in a world that I am old enough that we had separate networks, I think the reliability when things like 9/11 and tsunamis happen, the benefit of having multiple networks and the Internet outweigh the needs of a protected, isolated network because I don't believe in today's world that is a real answer.

Mrs. CHRISTENSEN. I don't have any other questions, Mr. Chairman. I will yield back the balance of my time.

Mr. WALDEN. I thank the gentlelady for yielding.

I believe Ms. Blackburn is next for questions. Then I will go to Mr. Shimkus next.

Mrs. BLACKBURN. I will skip.

Mr. SHIMKUS. Thank you, Ms. Blackburn, and thanks for the panel. Sorry, we have two competing panels, and I apologize for not hearing all the testimony.

Let me go to Mr. Lewis. You mentioned in your written testimony the importance of domain-name system security, DNSSEC. Could you describe the problem with the current implementation of domain-name systems and why DNSSEC is important?

Mr. LEWIS. Well, I think what you have heard from all us is when the people who designed the Internet designed it as a DOD network and then they thought it would grow out a little bit. They didn't worry about trust. They didn't worry about authentication. Phyllis knew it was her sister at the other end, right? When we did this, we didn't have to worry about this and so the domain-name system, which is the addressing system, is vulnerable to spoofing. It can be manipulated and, I think as you have, redirect traffic. So you think as far as you can tell on your machine you are going to a legitimate site and it could instead be the government of Iran or a Russian cyber criminal. You can spoof it. And DNSSEC uses authentication technologies largely so that we reduce that ability, really almost eliminate it, to impersonate another site.

Mr. SHIMKUS. Yes, and I think the challenge with this committee is, it is so high tech, so—you know, we are laypeople for the most part. It is just very tough for laypeople to understand. That is why we have experts like you come. A lot of us do understand domain, just the basics, why you have a domain. Now ICANN is exploding domain names, and with that, should we—and this is one for the whole panel—should we be working with ICANN to roll out DNSSEC?

Mr. CONNER. I think everybody is already working that. I would tell you be aware of newfangled toys. DNSSEC has a promise but it also has liabilities today that are equal to the liabilities we have today. Will it be there in 5 to 10 years? We hope sooner, but it is not there, not even close. I think we have got to use the capabilities we have like EBSSL where the chrome turns green and you know you are safe, and when someone says your identity is who it is, it is, and I think that is where I put the focus instead of buying $19 authenticate technology to take a responsibility liability for your identity and who that is, and if it costs you 500, I mean, that is where a bully pulpit starts to make a difference in our technology.

Mr. SHIMKUS. Mr. Dix, anyone else want to respond? Anyone else? That is fine, because I want to go to a couple other things. I also deal with democracy movements in former captive nations, eastern Europe, whatever you want to call them, and followed the cyber techs in Estonia years ago, the meddling by China and Russia and their neighbors and continue to be very concerned, although the new technological age is allowing democracy movements to get their word out, to communicate, and that keeps evolving. But you also see governments like the government of Belarus try to clamp down on that and which I have also been very concerned about. So that is just a statement. I mean, it just an evolving—it is like a competitive market. People want to get information but the bad guys want to get around and it moves too fast that we can really regulate. I have always said that about this subcommittee and the tech community, there has got to be a lot of self-interest that gets people to move before they get caught.

Let me just segue real quickly into, I serve on the Energy Committee and we go to power plants all the time. I am a big proponent of nuclear power. And Mr. Terry's opening statement talked about, well, you could be secure if you just had a desktop alone and were no longer connected. Now, with WiFi and stuff, who knows what folks could end up doing. But the power utility system relies so much on data going to RTOs, really what they are producing is excitable electrons to get on the grid, which if that all we had to worry about and had a closed system, we would be fairly safe, but it is all the monitoring and calculation of the load. What is the solution to the utility industry? Does anyone have——

Mr. CONNER. Two thoughts. One is, as I testified earlier, that is why you have to start with DOE's elite. Electrical is very different than nuclear at the source. We believe you have got to start within the power production plant itself. We are working with large manufacturers in terms of how do you authenticate everything in that power production plant because you want to know what parts, whether they are original ones or the alternate parts coming in, who they are and where they are from. And frankly, that doesn't matter whether they come from good or bad sources, just know where they come from and that they are there.

The second thing we then focus on is, who is accessing those systems and sharing that information so only the people with the right authorization or identity can see it. And then the third thing we are working with them is, how that data is shared because data, in and of its own, at one location will not solve a grid by definition.

Mr. LEWIS. Two other quick points. The idea of a secure network, a standalone secure network, just doesn't make any sense. People bring their iPhone to work and they plug it in to charge, and we have seen that happen twice with allegedly isolated air gap networks, so forget it.

We need to think about securing the industrial control systems, the SCADA networks. This is an avenue of attack. It is a different kind of network technology. Right now, it is the typical thing. When you buy it, the password is "password" and the user name is "admin" and it doesn't take a lot of activity for foreign opponents to figure that out. People also need to look at how their critical infrastructure connects to the Internet. When you talk to nuclear companies, for example, they will usually tell you we are not connected. When you do the actual survey, what you find is, you know, sure, so we need to have some way to bring the industry—some companies do great. Others need some help and we need to figure out how to do that.

Ms. SCHNECK. And one point on that, the good news is, a lot of these industrial control systems are the same across sectors so if you can get some best practices and some incentives in one sector, they will multiply across from the grid to even transportation and nuclear in some cases. Authentication is one vector. Another is what gets executed. It goes back to the instruction. It is a malicious instruction from someone you don't want going to execute on a system that talks to something that controls physical infrastructure, and that comes from working at the component level, making sure that you have technology in those components that looks at whatever operating system is on that and says only execute these things. This is actually pretty simple on these because they only do one job in life. They are a component on the SCADA system. It is not just—it is not like they are a big server so you can lock down what they do.

Mr. SHIMKUS. Thank you, Mr. Chairman. Thank you.

Mr. WALDEN. Thank you.

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

Mrs. BLACKBURN. Thank you, Mr. Chairman, and thank you all for being here and for your patience with us.

I want to say just a couple of things. I think it is so important that the industry lead on this. Anything that we do, as different members have said today, is going to be passé before the ink is dry on whatever it is that we do. As we look at the security issues, I think that your guidance is there.

Another thing. We have spent some time in this committee and also in CMT, Commerce, Manufacturing and Trade, looking at the issue of privacy and the data security issue, the breach notification issue, which is a component of what we have here, and quite frankly, I think that most people do not realize the vulnerability that exists in their home with the computer that is there, and believe you me, I hear about it a lot with my district in Tennessee with all the songwriters and entertainers and the individuals that are in logistics informatics or financial service informatics or health care informatics and auto engineers. So the problems are compounding for this every day. But as we look at the privacy issue and in my conversations with them, let me ask you about Federal preemption.

And as we look at our standards on breach notification, data security, I wonder if you all have any thoughts on putting in Federal preemption language and making certain that we are working from one standard and the importance of that.

Mr. CLINTON. Ms. Blackburn, if I could, we are supportive of Federal preemptive notification requirement. I think we have 47 different ones now. For a multi-state company, it is very, very difficult to work on the similar themes that I have been hammering on throughout today and generally is that we have to understand that it is not a technical problem, it involves cost. If we can find a way to reduce cost, we can have good standards but we don't have to have multiple good standards. So we can lower compliance costs, increase simplification, we will have better adherence, we will have better security, better privacy and at lower cost, and I think that that ability to cut through kind of the government falling all over itself at the various levels is critical to getting that done, so I am very supportive of that.

Mrs. BLACKBURN. OK.

Mr. CONNER. I would second that. I would tell you the single largest legislation issue that has brought security from being in the Stone Age to today is probably California 1386. Why? Because it said if it happens, you have a carrot and a stick. If you tried to protect yourself with encryption, you are safe, and if you haven't, you are liable for a class-action suit. That is singly the shot that was heard around the world, at least in the United States. The problem being, as Larry said, we have got too many State legislations, a patchwork, so that needs to get dealt with because it is an inextricable link to cybersecurity in terms of that.

The second piece I would tell you is the regulation that just was passed by the FCC about disclosure is going to have just as profound impact. The problem is, it is only public companies, and that disclosure is pretty nebulous in terms of being meaningful for you as a small business person in Knoxville or Nashville or Memphis in terms of what that means to you.

Mrs. BLACKBURN. OK. Thank you. I will yield back.

Mr. WALDEN. The gentlelady yields back, and now I think our final questioner is Mr. Bilbray from California. We welcome your comments. You are recognized for 5 minutes.

Mr. BILBRAY. Thank you, Mr. Chairman.

Mr. Conner, do you believe that law enforcement has the tools they need to go after cyber criminals as described in your testimony?

Mr. CONNER. No, they do not. I have to tell you, if you look at the attempts that are being made with DHS and within Justice to have the criminal network geared up, I mean, part of the problem is, we look at it and there are one-time uses for critical events. Well, unless you use it every day, that system is never going to be ready. We partnered with Interpol to do just that. They have 6,000 agents worldwide, and their issue was—because I certainly didn't have the money—Interpol is treated like a country now under passport control. We were able to put their passport information so it has biometrics. Unfortunately, this country doesn't deal with that in its passport today. It is first generation digital. The second thing it has—and this is all on commercial chips—it has software to do

logical access so those 6,000 agents if they go after a tsunami, they can go on any network, including an Internet cafe, and be secure in getting access to that information, whether it is mobile, etc., and last but not least, physical access to every Interpol office. All that technology resides on this little card—this is a real one—that those 6,000 agents use around the world today as they follow crime, hopping jurisdictions that have three different standards, three different use cases, that allows them to do their job. Why is it important? Because it is what he or she has to use every day. To the extent it is not something you use every day, it will not be useful at the time of need in some event.

Mr. BILBRAY. So basically you are saying we are at place in cyber crime where we were in the 1930s with the bad guys running around with Thompson submachine guns and the cops carrying .38 revolvers.

Mr. CONNER. Well, and worse than that, we are isolated. We are isolated here in the United States with, as my colleague said, the most at risk and no ability to interwork on a global capability with the good guys to defend that.

Mr. BILBRAY. It is interesting you bring that up because I think that most of us here will remember after 9/11 this issue of the technology, security, the biometrics, the high-tech stuff was one of the top priorities of the 9/11 Commission. We passed a thing called the REAL ID bill and now everybody has found excuses to keep dragging it on, dragging it on. In fact, I think we are even giving grants to States for homeland security and States are refusing to implement the 9/11 recommendations, so we are giving them money and they basically say that we want to spend it on other things rather than the first priorities. Do you think we may want to revisit that whole situation rather than just ignoring the fact that——

Mr. CONNER. Absolutely. I spoke the morning after Bush addressed both the House and Senate. That morning after, I was with Mr. Bennett and other legislators that were leading this effort and spoke at NATO after 9/11 on, we have learned to defend air, land and sea, the next frontier is cyber. Unfortunately, in those 10 years, we made a lot of progress but the bad guys have made more progress and they can jump across jurisdictions with no legislative legal barrier.

Mr. BILBRAY. Mr. Chairman, I have to say that this is one thing that I think that our committee always referred over to Homeland Security but here is a point where we may want to talk. This is a place that both sides of the aisle should be able to cooperate on. We have got a consensus there. And frankly, the bad guys in here, the obstructionists are on both sides of the aisle too. So maybe this committee can take a look at, you know, how we can go back and revisit that and address that issue.

And I appreciate the fact that you draw the line about—I am concerned and I will ask the doctor to jump in here because the two at the end brought up two interesting things, that when we develop strategies, how to address this. We don't want to create a box that gets people to litigate the private sector but we also don't want to create a box that allows the bad guys to know how far they have to move outside to avoid it, and I would solicit both comments. Let us start with the doctor and then I will go back of how, you know,

can you elaborate again how that us creating arbitrary boxes may be utilized by the bad guys.

Ms. SCHNECK. I think it was said earlier, and even by Ranking Member Eshoo, this issue is so vast, this is science, that if you start saying you will implement these five things, the adversary is always looking at how to get around that. They know their target. They know what they want. They spend many months and people on finding exactly the intellectual property they want. They find the person and the company. They know what the person will respond to and they get it.

It is quite clear that if we say we are going to seal up these gateways and these ways, these are the best practices that we must follow when it is a regulation, that is where the money will go, and after that, the money won't go to anything new and different and therefore the adversary then always goes outside that and says well, I can get in this way. It is like the point to the industrial control system. They say they are disconnected but true story after true story finds a little modem out the back so the person can watch the game while they do the monitoring. There is always a way out in science, and what we want to do is instead incentivize. You have a classic problem. We are not incentivized to do what is good for the greater good. We are incentivized towards our shareholders. So instead, if you put that money and that incentive toward innovation, we will end up building stronger and better technology at many times the speed that the legislation could even get through do to the, quote, protection.

Mr. CONNER. Congressman, I think that is a great question. I am frankly less concerned about what we say we are doing. Say anything you want, by the time you say it, they have already figured that out. They are not waiting for us to legislate and regulate and figure out the next hole. I think the model is very clear. It is joint forces and it is in DOD. We still have strong Army, Air Force, Marines, Colonel Garlick, and they act on their own. They are highly integrated with their suppliers. There is what is publicly available. I served on the Joint Forces Advisory Board as a private sector person. There is what you do in that that is public and there is what you do that is not public, and I think that is how cybersecurity has to be treated. There was 10 percent of the money set aside to deal with cybersecurity, and no Army, Air Force department could do. They had to get their best and brightest in on it and they had to share what is public is public and what is not public is equally or maybe more important.

Mr. BILBRAY. Thank you, Mr. Chairman.

Mr. Chairman, they referred to Australia. Being the son of an Australian war bride, it reminds me of the story of a notorious Australian bushman, a robber named Ned Kelly. Ned Kelly was notorious for putting so much armor on so that nobody could shoot him, and his armor slowed him down so much that they shot him in the back where he wasn't armored, and I think that may be very symbolic of the Ned Kelly syndrome, that we put on so much armor thinking we are defending and what we do is create an opportunity for the bad guys to get around it.

Thank you. I yield back.

Mr. WALDEN. I thank the gentleman and I thank all our committee members for letting us have a more freewheeling hearing than sometimes we have, but the value of the content we got from you all is just unparalleled, and I think my colleague, Ms. Eshoo, and I will be reaching out to each of you to say come back to us with what really would work. We got a lot of that today and our staff has got that. We are going to move forward on this. I think there is an opportunity to look at device manufacturers, perhaps the phone side, the router side, there is an issue on the education side, and so we really appreciate what you are doing out there in this fight and your input to us so we can try to get it right and solve this problem.

With that——

Ms. ESHOO. I would say bravo and thank you very much. Every member really drew so much from your testimony and the answers to our questions have been most, most helpful. Thank you.

Thank you, Mr. Chairman.

Mr. WALDEN. Thank you, and with that, the committee will stand adjourned.

[Whereupon, at 11:56 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Communications and Technology Subcommittee Hearing
Cybersecurity: Threats to Communications Networks and Private-Sector Responses
By Rep. Cliff Stearns
Wednesday, February 8, 2011
(155 words)

Thank you, Mr. Chairman.

In preparing for today's Hearing and listening to a variety of stakeholders, including the witnesses here today, I am struck by a number of themes.

First, it is clear that we have a cybercrime problem. Our efforts in assuring cyber security are simply not keeping pace with the advancement and proliferation of cyber threats. And, importantly, the most common victims of targeted cybercrimes are small businesses.

Understanding this problem, there are several solutions put forth by private industry. Specifically, rather than applying antiquated, heavy-handed regulations we must work together with the private industry and provide incentives for investment and innovation in the area of cybersecurity. We should also dedicate our resources to enhancing consumer education so that our constituents are able to fully protect themselves.

Therefore, I thank the Chairman for calling this Hearing and look forward to continuing to learn how we can best protect our constituents and our country from future cyber attacks.

Statement of
Representative John D. Dingell
Committee on Energy and Commerce
Subcommittee on Communications and Technology
Hearing on "Cybersecurity: Threats to Communications Networks and Private-Sector Responses"

February 8, 2012

Mr. Chairman, thank you for holding this important hearing today. I am not alone among my colleagues in recognizing that growing interconnectedness has brought with it new security risks that require well-reasoned responses. In the past year, computer hackers have infiltrated the networks at both CitiGroup and Sony. Additionally, RSA Security, which manufactures the SecureID tokens used by many federal employees also had its security compromised in a recent attack. Moreover, we have all read about Chinese hackers attacking the Pentagon. In short, these attacks are serious reminders of the vulnerabilities in our private and public communications systems and the pressing need to address them.

Although most recent cyberattacks have been commercial in nature and were carried out by hackers seeking to make a profit through espionage, those who seek to do our country harm could soon turn to a cyberattack to accomplish their aims. Our utilities, communications networks, and financial system are all currently at risk. As Mr. Lewis notes in his testimony, a recent U.S. Department of Homeland Security study indicates that most critical infrastructure companies had been penetrated by a cyberattack at least once. Such vulnerabilities are real and could allow terrorists to do great harm to our way of life using only a computer.

I hope this hearing will be a useful starting point for the Committee. There are several pieces of legislation moving through Congress which address the issue of cybersecurity, and each takes a different approach to the problem. However, it is clear that there needs to be more cooperation and collaboration between the private sector and the federal government to protect the country's critical infrastructure. I would also implore my colleagues to approach this problem reasonably, with an open mind, and a willingness to compromise. We live in the 21st century, and achieving a 21st century solution will require bipartisan cooperation.

In closing, our national security requires that we competently address cyberthreats. As the Internet and the nature of communications continue to evolve, adaptable solutions to the pernicious problem of cybersecurity must be found and agreed upon. I urge my colleagues to take heed of this and show their constituents we can stop bickering for a moment to address a problem that has the potential to touch every American.

Thank you for your courtesy, Mr. Chairman. I yield back the balance of my time.

The Committee on Energy and Commerce

Internal Memorandum

February 6, 2012

To: Members and Staff, Subcommittee on Communications and Technology

From: Majority Committee Staff

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

The Subcommittee will hold a hearing Wednesday, February 8, 2012, at 9:30 a.m. in 2322 Rayburn House Office Building entitled "Cybersecurity: Threats to Communications Networks and Private-Sector Responses." The hearing will examine threats to America's communications networks, what the private sector is doing to address those threats, what the private sector could be doing better, and what role the federal government should play. One panel of witnesses will testify.

I. Witnesses

Larry Clinton
President and Chief Executive Officer
Internet Security Alliance

Robert Dix
Vice President of Government Affairs
& Critical Infrastructure Protection
Juniper Networks

Phyllis Schneck
Vice President and Chief Technology
Officer, Global Public Sector
McAfee Inc.

Bill Connor
President and Chief Executive Officer
Entrust

James A. Lewis
Director and Senior Fellow,
Technology and Public Policy Program
Center for Strategic
and International Studies

Additional witnesses may be called at the discretion of the Majority.

II. BACKGROUND

Americans are more interconnected today than ever before. Communications networks empower our citizens to share information across the country in the blink of an eye. The Internet

has become an essential component of our economy, and now also supports vital infrastructure such as power distribution and our transportation networks, as well as services such as medicine, finance, and education.

Emerging Vulnerabilities.—Our growing interdependence has also exposed the vulnerabilities of our communications networks, as bad actors exploit the open protocols of the Internet for financial, political, and military gain. While the general public has become aware of Trojan horses, spyware, viruses and other malware that affects computers, the vulnerabilities of communications networks are even more complex and cyberattacks are becoming more prevalent and more sophisticated. When hundreds or thousands of computers are infected by the same malicious software, the bad actors behind that software can transform that collection of computers into a botnet. With a botnet, a hacker has a powerful tool to take down websites through distributed denial-of-service attacks, to hack into protected networks through brute force, and to distribute illegal and unwanted content. With the capability of simultaneously transmitting large amounts of data from thousands of points at one time, botnets possess the capacity to bring down communications networks, at least where those networks are capacity constrained. Even without a botnet, the lightning-fast speeds and global nature of modern networks means that bad actors have more opportunities to exploit weaknesses in network defenses than ever before.

The physical components of communications networks are another potential vulnerability. With trade becoming increasing global and supply chains increasingly complex, the opportunities for misfeasance and malfeasance within the supply chain network has dramatically increased. Communications network providers purchase networking equipment from manufacturers who in turn outsource the production of chipsets, processors, and other components to others. Weakness can occur at any point in this supply chain, and the costs of overseeing each and every stage of production may be prohibitively expensive. The increasing reliance on wireless communications may create another vulnerability as consumer wireless devices become an additional access point into the network.

The Internet's architecture may itself create vulnerabilities. For example, in 2008, network researcher Dan Kaminsky discovered a flaw in the implementation of the Internet's Domain Name System (DNS), the system that translates human-readable domain names into the machine-readable IP addresses. A bad actor could exploit this flaw to perform a man-in-the-middle attack on a consumer—with such an attack, a consumer thinks his username, password, and financial information are securely transmitted to his bank when in fact the bad actor sits in between the consumer and his bank, able to see all the information transmitted between the two. The discovery of this vulnerability prompted the development of DNS Security Extensions (DNSSEC) as means to prevent such attacks, although DNSSEC's effectiveness depends on its widespread adoption by ISPs and websites. Similarly, the evolution to the next generation of IP addresses, known as IPv6, and the continued expansion of domain names may create new vulnerabilities and obstacles to effective law enforcement.

The Continuing Cyberthreat.—The evidence of the last few years has shown that the threat to communications networks, the threat of persistent cyberattacks for purposes of crime, espionage, agitation, and even warfare is real. Attempted cyberattacks on federal government networks have increased year after year with a double-digit rate of growth. In October 2010, the discovery of the Stuxnet virus demonstrated the ability of a well-placed virus to disable critical

infrastructure—in that case nuclear facilities. According to Symantec's 2011 State of Security report, 71 percent of companies experienced some form of cyberattack in the past year; and according to a joint study by Verizon and the U.S. Secret Service, there was a comparatively huge increase in the number of external cyberattacks against American business and government.

The sources and motivations behind cyberthreats are numerous. Perhaps the most common are cybercrimes, like identity theft, credit card fraud, and online piracy. Bad actors can exploit malware like the Zeus virus to trick consumers into authorizing fraudulent bank transfers. Online forums foster a black market in stolen credit card and social security numbers, which are often traded in blocks of one thousand or more. The accessibility of private information about individuals online has made companies and individuals more susceptible to social engineering—the practice of tricking individuals into revealing sensitive information using information already known about the individual. Private estimates of the cost of cybercrime range in the billions of dollars each year, a continuing tax on online commerce and innovation.

Cyberagitation is a newer form of cyberthreat. With cyberagitation, the motivation of the cyberattack is often political, not financial, as seen most prominently this past year with the attacks by "Anonymous" on financial organizations in response to the WikiLeaks controversy. Just last month, "Anonymous" launched cyberattacks on the U.S. government, the Motion Picture Association of America, and several other groups in response to anti-digital piracy efforts. Aside from the damage the cyberagitation may do to businesses and our virtual infrastructure, the methods used by cyberagitators could be used to carry out cyberterrorism if done on a massive scale or aimed to incite panic and confusion. What is more, cyberagitation may feed cybercrime—cyberagitators may, for example, purchase access to a botnet or malware in order to carry out their political ends.

Cyberespionage remains a continuing threat to both commercial and national interests. Bad actors, either of their own accord or sponsored by hostile foreign states, may view cyberspace as a new domain to infiltrate American corporations to steal intellectual property and trade secrets. Those same actors may see cyberspace as a cheaper alternative to traditional spycraft. In the 2008 presidential election, for example, bad actors breached the computer networks of both major party candidates. Perhaps even more concerning, classified information at the Department of Defense was breached in 2008 via a virus hidden on a flash drive—it took the Department nearly 14 months to remedy the situation.

Finally, cyberwarfare is most commonly seen in the threats to critical infrastructure that could occur online. A major disruption to a large bank could trigger another financial crisis; a cyberattack on the core components of the communications network could disrupt all Internet-enabled communications including interconnected VoIP service. And such disruptions need not be based online—supply chain vulnerabilities, terrorist attacks, or even a natural disaster could compromise our communications networks. Although the United States has not experienced a catastrophic Internet failure, there have been online and physical incidents that caused localized and regional disruptions.

One Lincoln Centre
5400 LBJ Freeway
Suite 1340
Dallas, Texas 75240
(972) 728-0447

Tuesday, March 20, 2012

The Honorable Greg Walden,
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
2182 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden,

Thank you again for the opportunity to share my global knowledge and experience on Cybersecurity with your committee. The questions that were submitted to me definitely indicate that the committee clearly understood the content, and are eager to take action. I have answered all of the questions, and I realize that further detailed discussion and follow up is probably required for some of the items. Please let me know how I can help further, and I will make myself and my team available as required.

Bill Conner

The Honorable Greg Walden

1. Mr. Lewis mentioned in his written testimony that the government could play a coordinating and incentivizing role regarding the widespread adoption of Security Extensions for the Domain Name System, also known as DNSSEC. Do you agree, and if so, what should the government do specifically?

    - DNSSEC deployment has been very slow for number of reasons. The two leading reasons are that it's not beneficial without a widespread deployment, and enterprises that adopt it do not realize any immediate gain. These types of users will typically deploy technology that provides them immediate and significant benefits. Secondly, it requires a good deal more server resources to provide the security extensions because it has to handle much more information which reaches maximum capacity very quickly.

      In addition, the Congress can help with DNSSEC deployment. An easy and effective thing for the Congress to do is lead by example. It would be appropriate and show leadership for Congress to implement DNSSEC in the Congress's own Internet presence. In this, and other cybersecurity issues, Congress has its own need to have an infrastructure that is among the world's best. Congress also has a top-notch IT team, among the world's best. By implementing world-class security Congress can display what can be accomplished and set a tone for greater adoption.

2. Mr. Clinton in his testimony mentioned the formation of an "underwriters' laboratory" style information clearinghouse for cybersecurity. What do you think about that idea? Would sharing additional information with cybersecurity insurance providers, perhaps through private-sector clearinghouses and with appropriate privacy safeguards, help foster the development of such a program?

    - An "Underwriters' Laboratory" style information clearinghouse for cybersecurity is definitely a good concept, but a lot of this framework already exists today within the U.S. Department of Commerce, under the NIST Computer Security Division. NIST has developed standards and certification programs for cybersecurity products and processes. Cybersecurity is not a one time, Y2K type of issue. The threat landscape is constantly changing and so must the manner in which you address these threats. The NIST standards and programs address this issue since they are constantly being monitored and updated as threats evolve. We believe that this program can be leveraged in a Public/Private partnership to provide the proper cybersecurity education and guidelines. We also support each agency working directly with their current industry partners and counterparts. This information can still come together in one "clearing house" location, but each discipline should work in their area.

3. Several members of the panel highlighted the need to remove legal impediments that may prevent Internet service providers, cyber security software providers, and others to address cyber-threats and share information. Could you identify any specific federal or state laws, regulations, or other legal impediments that Congress can address to improve cyber security?

    - There are a number of statutes that inhibit the sharing of information among actual or potential competitors and these can also inhibit sharing information of security breaches. The Sherman Act discourages communications with competitors that may constitute price fixing or market allocation or similar anticompetitive activity. FERPA, HIPAA and Gramm Leach Bliley are all federal statutes that protect privacy, but they also have the effect of discouraging communication about security breaches if the information at issue is the type protected. Moreover, typical business is enmeshed in a web of contracts with it suppliers and customer, all of which may have confidentiality terms limiting disclosure of information related to those parties. Disclosure is the opposite of privacy and with numerous sources of privacy obligations, it is understandable that corporate counsel would be wary about any disclosure of information outside the corporation even if it is for the commendable cause of identifying a fixing possible security breaches .

    - There is a different dynamic in play when discussing information sharing between industry and the government. Industry has historically been willing to share information around threats and cybersecurity with the public sector. Unfortunately the public sector has been unable to share similar information in return, for fear of giving one entity a competitive advantage over another. I don't think there are any laws forbidding this type of two way communication; however, there are Government policies that prohibit the intelligence community from sharing this type of information. The sharing of information could, and should be set up so that all businesses and individuals could benefit from the content, while keeping the source of the content or information anonymous.

4. I have seen reports that indicate that many cybersecurity breaches could be avoided if businesses followed best practices. What are some of these techniques and how can we encourage more companies to adopt them?

    - Once again, the private/public partnership is essential. The FTC has already started to list best practices on a site called OnGuard Online. The purpose as listed is: **OnGuard Online provides practical tips from the federal government to help you be on guard against Internet fraud, secure your computer, and protect your personal information.**
      We could also see the SBA, Department of Commerce, and some other Agencies having an interest in publishing similar information. With the threat landscape

constantly changing it would be very easy for this information to become dated in multiple locations, and at varying stages. Referring back to our answer for number 2 above, the NIST programs should be utilized and each agency could then reference back to the best practices and solutions as identified under the NIST Computer Security Division.

One of the simple steps that we discussed during the hearing is for businesses to also ensure that software is updated to the latest release, that passwords and protections are utilized and set at an appropriate level, and that physical access to critical assets is also protected.

Building on a specific situation that I detailed in my testimony, if you are interested in adoption of best practices, I believe that, at a minimum, business should make sure their financial institutions have solutions that provide:

- Strong identity proofing, verification, and authentication
- Transaction verification and confirmation
- Real time Fraud Monitoring and detection

5. The Internet is currently transitioning from IPv4 to IPv6 addressing. Does that process create any new cybersecurity issues? Will transitioning to IPv6 alone solve any cybersecurity issues that currently exist? Does the process of transitioning to IPv6 present opportunities of resolve existing cyber security issues?

    - The IPsec transition does not create any significant new security issues. Similarly, it does not solve any significant new security issues, either. However, IPv6 does encourage the use of IPsec and this is a significant improvement for cybersecurity. IPv6 makes it easier to use other core technologies such as DNSSEC, and is thus an enabler of better cybersecurity. As you know, IPv6 is necessary due to the ever increasing number of IP devices in the network, and the possibility of rogue and malicious devices also increases. As these numbers continue to grow, it becomes that much more important to have known good devices identified and authenticated correctly.

6. In December, we heard from witnesses that the implementation of "WHOIS" databases makes it difficult for companies and law enforcement to identify and track down the owners of websites that are facilitating illegal conduct, including sites that host malware. What is the private sector doing to strengthen the use of WHOIS to help combat cybercriminals, and are there any steps Congress can take to facilitate that work?

    - There are already laws that require that a legitimate entity be listed in the WHOIS database. This stops the abuse of a WHOIS entry having a fake address such as "123 Main Street, Anytown USA." It enforces accuracy in the database. But this also

creates the situation where the legitimate entity is a broker for the real entity. In many cases, this is reasonably harmless -- the major registrars will be a broker for their customers for a small added fee. In other cases, the bad actors simply set up a shadow entity that shields them and they go on as before. The net result is that the good guys pay more and the bad guys still hide.

To be clear, international criminals, state actors who steal intellectual property, and other Internet "bad guys" are also enabled by an accurate WHOIS; it tells them who to hack. This is where the policy conundrum comes into effect. It is hard for Congress to enable legitimate law enforcement in a way that does not also enable Iran, China, and international criminals. That is a problem you will need to wrestle with further as you work on implementing the WHOIS database.

The Honorable Anna Eshoo

1. Several agencies, including the FCC have been exploring a voluntary, industry "code of conduct" as a way to address the detection and mitigation of botnets. Do you support such an effort and how do we ensure it's effective?

    - Through the proper administration of an Information Security Governance (ISG) framework, industry can definitely perform self-assessments of their company, processes, applications, and networks. Working as a co-chair of the DHS public/private committee on Cybersecurity, I led the effort to develop an ISG framework which we successfully followed and implemented in our enterprise. That effort developed an approach that will ensure companies stay current of threats and ensures that someone is actually in charge of ensuring compliance within an entity.

      We continue to successfully use this self-assessment framework today from a security and continuity of operations perspective. That said, too many enterprises have not embraced this approach and need to be encouraged to utilize such tools. One such approach could be that the ISG recommendations could be overseen by the government and then enterprises that follow these guidelines could advertise that they follow this governance framework as a means of best practices. That may encourage broader compliance.

2. Access to secure data and cloud services over mobile networks is essential for the government and large enterprises. Are there unique threats designed to attack vulnerabilities in our wireless networks? Is there a weakness there that needs to be strengthened?

    - There are threats out there today regardless of the communications network or transport medium being used. With the introduction of cloud computing, the type(s)

of network being used cannot be guaranteed or defined. For this reason, we should not focus on the ISP's or communication networks, but on the underlying identities and security. It will be important to have strong identities and authentication (make sure the party your interacting with is who they say they are), and to make sure that the content is protected either with data encryption or over SSL.

3. Your testimony highlights "ZeuS" or "SpyEye" as a growing threat for mid- to small-sized companies. What near term steps do you recommend businesses implement to prevent these types of breaches and what do you recommend that we, as Congress, do to protect these businesses?

   - Small Businesses need to make sure that their financial institutions have implemented strong identity based security with transaction verification and fraud detection before banking on line. Short of that, there are some things they can do internally to help mitigate the risk of banking online :
     - Have a dedicated computer for on line banking. This computer cannot be used for any other internet traffic or browsing, and it should be disconnected from the internet when not being used for a banking session. This computer should not have any external drives or disks connected to it at any time.
     - Self-assessment and remedies using an Information Security Governance framework to ensure proper security and continuity of operations.
     - Proper security awareness training of employees to ensure proper security guidelines are followed, and to avert opening of malicious links and social engineering attacks.
     - Ask financial institution what they are doing for identity based security, transaction verification and real time fraud monitoring, and act accordingly
     - Must understand their contractual liabilities with both their customers and financial institution for the various States which they conduct business in.

The Honorable Henry Waxman

1. The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) has been formulating recommendations for best practices to ensure optimal security and reliability of communications systems. How do you see this process contributing to improvements in cybersecurity?

   - There are threats out there today regardless of the communications network or transport medium being used. With the introduction of cloud computing, the type(s) of network being used cannot be guaranteed or defined. For this reason, we should not focus on the ISP's or communication networks, but on the underlying identities and security. It will be important to have strong identities and authentication (make sure the party your interacting with is who

they say they are), and to make sure that the content is protected either with data encryption or over SL.

2. What opportunities do you envision for government and industry to work together towards coming up with critical cybersecurity solutions? What role specifically do you see for the FCC?

    - We fully support a private/public partnership for cybersecurity information sharing that is actually a two-way street. Each agency working directly with their current industry partners and counterparts is the best solution since those relationships are trusted and exist today. This information can still come together in one "clearing house" agency, but each discipline should work in their area (for example: DOE and Energy companies). The consolidated data can then be shared equally across industry and the sources remain anonymous.

The Honorable Bob Latta

In your testimony, you mention that you need a "layered, identity-based security" solution. Can you expound on what you mean by "layered" and "identity-based"?

- Today's criminal groups, as well as the malicious tools they deploy, have evolved to a point where a single security layer is no longer adequate to properly safeguard critical information, identities or access to buildings and networks.
  By implementing several proven security layers — for example, strong username and password coupled with a grid card, one-time-passcode (OTP) token and device authentication —organizations are able to critically reduce the severity and success of attacks from malware, breaches, viruses or social engineering.
  This layered method is even more effective when organizations are able to leverage strong authentication from a single management platform. This approach provides the ability for organizations to migrate to new authenticators, in real-time, during an attack. Recent high-profile breaches of major security vendors have shown the disastrous end-result when corporations are tied to a single authenticator — without any recourse in the event of an attack.
  This layered method also is complementary to identity-based security, where every device, user, machine or application possesses a digital identity that must be properly verified, authenticated and protected. Organizations, enterprises and even governments will never achieve 100 percent assurance of a transaction or communication without authenticating the identities on both ends.

Identity-based security solves this challenge by providing software-based platforms that issue, revoke, manage and authenticate necessary digital identities. These digital identities are necessary for everything from an employee to a mobile device, water meters and medical equipment in hospitals. Identity-based strategies are the most advanced security initiatives and are at the forefront of strong authentication, as well as mobile- and cloud-based security.

20 March 2012

The Honorable Greg Walden
Chair, Subcommittee on Communications and Technology
U.S. House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

RE: February 8, 2012 Hearing Questions for the Record

Dear Mr. Chairman:

As you are aware, I testified before your Subcommittee at its February 8, 2012 hearing entitled "Cybersecurity: Threats to Communications Networks and Private-Sector Responses." On March 6, 2012, the Subcommittee transmitted to me questions for the hearing record from its members. Please find attached my responses to these questions.

Should you require any additional information, please feel free to contact me at (571) 203-2687 or rdix@juniper.net

Sincerely,

Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection

Enc.

cc: Hon. Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

JUNIPER NETWORKS
2251 Corporate Park Drive
Herndon, VA 20171
o +1 571 203 1700
f +1 571 203 1790
www.juniper.net

QUESTIONS FOR THE RECORD
Bob Dix, Jr., Juniper Networks
House Subcommittee on Communications and Technology
February 8, 2012

QUESTIONS POSED BY THE HONORABLE GREG WALDEN

1. **Mr. Lewis mentioned in his written testimony that the government could play a coordinating and incentivizing role regarding the widespread adoption of Security Extensions for the Domain Name System, also known as DNSSEC. Do you agree, and if so, what should the government do specifically?**

   DNSSEC is an important tool in securing the infrastructure. The FCC has an initiative to expand adoption of DNSSEC. Juniper has expressed support in writing for the efforts of the FCC.

2. **Mr. Clinton in his testimony mentioned the formation of an "underwriters' laboratory" style information clearinghouse for cybersecurity. What do you think about that idea? Would sharing additional information with cybersecurity insurance providers, perhaps through private-sector clearinghouses and with appropriate privacy safeguards, help foster the development of such a program?**

   The notion of insurance as a tool in managing the risk association with cyber security has merit and the market has been developing such products for some time.

   In terms of information sharing, as it regards cyber security the discussion at times fail to properly reflect the objective. Information sharing is a tool to achieve situational awareness and a common operating view of the cyber domain in order to improve detection, prevention, mitigation, and response to cyber events that may become incidents of national consequence.

   Much work has been done on this topic, but much work remains, including a focus on a national capability that recognizes the global elements of the issue. In May 2009, the President's National Security Telecommunications Advisory Committee (NSTAC) recommended to the President the establishment of a joint, integrated, public–private 24 x 7 operational capability to address this challenge. The recommendation laid out a multi-phased approach to achieving this capability. That effort was followed by a private sector initiative to build and pilot a capability to share, correlate, and analyze information related to malicious and abnormal cyber activity. This included the construct of a relevant legal agreement; concept of operations; standard operating procedures; and measures of success.

A follow up effort to integrate the effort with the Department of Homeland Security met legal challenges and was not successful in meeting the goal for the succeeding phase.

There are other efforts that have been conducted or are currently underway that are able to contribute to such a national capability. An effort to examine the various lessons learned and converge the various elements, while working to identify technology, legal, and policy gaps would be an important step to achieving a national weather service-type capability that would enhance situational awareness in real time or near real time in a steady state and during times of escalation, in order to issue appropriate alerts and warnings; recommended protective measures; and timely intelligence to improve detection, prevention, mitigation, and response to cyber events that may become incidents of national consequence. It is about managing risk and improving the cyber protection profile of our nation in a global context.

3. **Several members of the panel highlighted the need to remove legal impediments that may prevent Internet service providers, cybersecurity software providers, and others to address cyberthreats and share information. Could you identify any specific federal or state laws, regulations, or other legal impediments that Congress can address to improve cybersecurity?**

In general, technology companies are concerned with triggering liability under a variety of laws if we share cyberthreat information. For instance, threat information that is identified from the electronic communications of a communications customer might be protected from disclosure by electronic communications privacy laws. Companies also are concerned about violating their obligations to shareholders and customers by disclosing to the government or business competitors what could be viewed as proprietary information or information that could have a negative impact on the company if disclosed.

With this in mind, legislation introduced by a Member of this Subcommittee, which you have cosponsored, would amend the National Security Act to facilitate the sharing of cyber threat intelligence with eligible private sector entities. Rep. Mike Rogers (R-MI) introduced H.R. 3523, the "Cyber Intelligence Sharing and Protection Act of 2011," in his capacity as Chair of the Permanent Select Committee on Intelligence. The bill protects the sensitive nature of such information by requiring that security clearances be granted as necessary to the relevant private sector entities. In addition, the bill ensures that that the private sector treats the sensitive information as such – private sector recipients of the threat information may use it only to protect rights and property. Finally, the bill confers liability protection for companies that choose to protect their networks or share information based on the authorities provided under the bill.

4. **I have seen reports that indicate that many cybersecurity breaches could be avoided if businesses followed best practices. What are some of these techniques and how can we encourage more companies to adopt them?**

The cyber threat is no longer limited to an office network or work persona. Adversaries realize that targets are typically more vulnerable when operating from their home network since there are fewer rigors associated with the protection, monitoring, and maintenance of most home networks. Home users need to maintain a basic level of network defense and hygiene for both themselves and their family members when accessing the Internet, including using strong passwords to protect Internet connections, using updated virus and malware protection software, and opening only trusted websites and e-mail/e-mail attachments.

For enterprise networks, basic cyber hygiene must include fundamental network security management policies and procedure enforcement. These policies include, but are not be limited to:

1. Whenever possible, the enterprise must ensure that employees maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time.

2. Enterprise-wide wireless security devices, software and management systems must be in place to control and secure data transfers. Wireless access configuration management control settings must be utilized.

3. Many users do not exercise the same level of security on their home systems (e.g., limiting the use of administrative credentials). Therefore, home systems are generally easier to compromise. The forwarding of content (e.g., emails or documents) from home systems to work systems, and back, either via email or removable media put work systems at an increased risk of compromise. Security policies and procedures to filter and manage such content transfer must be in place and enforced.

4. Personal and business enterprise information, which traditionally has been stored on local or centralized computing and storage devices, is steadily moving to the Internet cloud.

    a. Examples of information typically stored in the cloud include webmail, financial information, as well as personal information posted to social networking sites.

    b. Information in the cloud is difficult to remove and is governed by the privacy policies and security of the hosting site.

    c. Corporate policy must address "Who will have access to the information being posted?" and "What controls does the enterprise have over how this information is stored and displayed?"

5. Corporate security policies should also include some form of application encryption to protect the confidentiality of sensitive information while in transit.

6. It estimated that 80% of cyberthreats can be prevented through the use of low-cost, even no-cost, solutions. Whether small or large, business cyber security policies must address access control, passwords and challenge responses. Internal and external users alike should be required to use forms of managed access controls to provide secure access to personal, protected enterprise or financial information. This can include password management, firewalls, and other readily available solutions.

5. The Internet is currently transitioning from IPv4 to IPv6 addressing. Does that process create any new cybersecurity issues? Will transitioning to IPv6 alone solve any cybersecurity issues that currently exist? Does the process of transitioning to Ipv6 present opportunities to resolve existing cybersecurity issues?

IPv6 is a welcomed advancement, but no panacea to cyber security. Implemented correctly, IPv6 can make for secure networks. However, before we reach the technical security circumstances of IPv6, we have to migrate to it first, and this migration may pose some security challenges. IPv6 is not inherently less secure than IPv4. IPv6 is a different protocol than IPv4. It is also a protocol that has not been "in the field" in any significant implementation. This could mean that there may be some challenges with v6 that we will need to address in addition to those currently in IPv4. IPv6 was specifically designed to be more flexible than IPv4 and this increased flexibility can create new types of security risks, if not addressed carefully. Juniper Networks has made significant investments in technologies and solutions that enable enterprises and service providers to meet mixed IP addressing needs even as they build out IPv6 networks as rapidly as markets and services require.

There will be a long period of transition in which networks need to support both IPv4 and IPv6 addressing. Juniper technologies provide a range of addressing techniques for traffic that has to flow between IPv4 and emerging IPv6 infrastructures. Coexistence of IPv4 and IPv6 cannot be addressed with a one-size-fits-all approach, but a toolkit of options based on the particular needs and configurations of current networks can provide the right solution. Transitioning to IPv6 alone will unlikely solve any cybersecurity issues that currently exist. Because there is no sizeable IPv6 content on the Internet, virtually all implementations will need to support both IPv4 and IPv6 for a relatively long period of time. No one knows how long this period will be where both will be supported. NIST has estimated that this "dual stack" way of internet address processing will be with us for as long as 20 years.

Industry is addressing this dual protocol issue through the use of network address translation (NAT), the process of modifying IP address information in IP packet headers while in transit across a traffic routing device. NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT has become a popular tool for alleviating the consequences of IPv4 address exhaustion. It has become a common,

indispensable feature in routers for home and small-office Internet connections and now service provider networks. Most systems using NAT do so in order to enable multiple hosts on a network to access the Internet using IPv4 addressing with common network processing functions. When bridging and transitioning between IPv4 and IPv6, you must take into account the specific set of security issues associated with both.

6. **In December, we heard from witnesses that the implementation of "WhoIs" databases makes it difficult for companies and law enforcement to identify and track down the owners of websites that are facilitating illegal conduct, including sites that host malware. What is the private sector doing to strengthen the use of WhoIs to help combat cybercriminals, and are there any steps Congress can take to facilitate that work?**

   Juniper is not in a position to address this issue.

7. **You mentioned in your written testimony that there are numerous private-sector organizations dedicated to cybersecurity, such as the Internet Consortium for Advancement of Security on the Internet and the Information Sharing and Analysis Centers. How do these private organizations contribute to cybersecurity? How, if at all, could the federal government facilitate their efforts?**

   As you indicate, my written testimony references SAFECode (Software Assurance Forum for Excellence in Code), ICASI (the Internet Consortium for Advancement of Security on the Internet), ISAC's (Information Sharing and Analysis Centers), SCC's (Sector Coordinating Councils), and the PCIS (Partnership for Critical Infrastructure Security) as private sector organizations dedicated to enhancing cybersecurity. In their own ways, each organization essentially facilitates the sharing of information related to network abnormalities, cyberthreats, operational capabilities, and security best practices.

   Unfortunately, the Federal government does not always share actionable information with these organizations in a timely fashion. For this reason, I believe Congress should pass legislation that facilitates government sharing of actionable threat information with industry on a timely basis. One example of such legislation, as I note above, is H.R. 3523 as introduced by Rep. Mike Rogers of Michigan.

QUESTIONS POSED BY THE HONORABLE ANNA ESHOO

1. **Several agencies, including the FCC have been exploring a voluntary, industry "code of conduct" as a way to address the detection and mitigation of botnets. Do you support such an effort and how do we ensure it's effective?**

   Juniper Networks supports voluntary, public-private initiatives to address the problem of botnets. In reference to the FCC, please see the attached letter that Juniper wrote complimenting the FCC's Cooperative Cybersecurity Initiative.

2. **Your testimony highlighted your company's significant investment in R&D and why additional investment in cyber security research is so important. How can Congress help encourage continued investment in this area?**

There are several ways in which Congress can encourage continued private sector investment in cybersecurity. One primary means would be to enact a permanent research and experimentation tax credit. As you likely are aware, Congress passes this tax credit as a temporary measure that is extended as it expires. In the most recent extension, the credit expired as of December 31, 2011, and does not apply to research expenditures made after that date. While it is possible that Congress could pass a retroactive tax credit in the future, this lag and uncertainty make it exceedingly difficult for businesses to plan their operations. Developing and implementing our plan for capital expenditures, research expenditures, manufacturing, investments, hiring employees, etc. is a constant function of our business; it is difficult to make a sound business decision when a major financial component is unknown. A permanent tax credit would provide businesses with the certainty we need to make continued, long-term investments in cybersecurity and other technological issues.

In addition, I believe that Congress could facilitate security research by not tying industry's hands through mandates or performance requirements. The fact that our customers are free to choose any security measure they deem valuable and useful is what drives Juniper to conduct significant research into developing new security technologies. If Congress passes legislation that requires our customers to choose from a menu of security options or otherwise regulates their choices, then the incentive to innovate beyond those options might no longer exist.

QUESTIONS POSED BY THE HONORABLE HENRY WAXMAN

1. **The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) has been formulating recommendations for best practices to ensure optimal security and reliability of communications systems. How do you see this process contributing to improvements in cybersecurity?**

As indicated in response to an earlier question, Juniper supports voluntary, public-private efforts to ensure the security and reliability of communications systems. In this regard, please see the attached letter that Juniper wrote complimenting the FCC's Cooperative Cybersecurity Initiative.

2. **What opportunities do you envision for government and industry to work together towards coming up with critical cybersecurity solutions? What role specifically do you see for the FCC?**

Please see the attached letter that Juniper Networks wrote in reference to the FCC's Cooperative Cybersecurity Initiative.

QUESTION POSED BY THE HONORABLE BOB LATTA

Can you expound upon the National Strategy for Trusted Identities in Cyberspace? How does this fit in with what Juniper is trying to do on cybersecurity?

Juniper has been actively involved in the evolution of the development of the National Strategy for Trusted Identities in Cyberspace (NSTIC) since its initial launch as the National Strategy for Secure Online Transactions. Those efforts have included work through the President's NSTAC on the issue of identity management and work through the Cross Sector Cyber Security Working Group to provide input to the NSTIC project. Juniper has significant subject matter expertise on the issues of security, authentication, access control, and more.

17 February 2012

Mr. Julius Genachowski
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: FCC/Industry Cooperative Cybersecurity Initiative

Dear Chairman Genachowski:

I write on behalf of Juniper Networks to compliment the Federal Communications Commission's (FCC) Cooperative Cybersecurity Initiative. Juniper believes that cybersecurity is a shared responsibility of government and the private sector and that managing risk will require a true collaborative approach between and among all stakeholders. In furtherance of this approach, we support voluntary industry efforts to better secure information and communications networks, and the Cooperative Cybersecurity Initiative takes a step in that direction.

The FCC's Communications Security, Reliability, and Interoperability Council has been working with service providers and other stakeholders to develop ways to identify, address, and mitigate network vulnerabilities. The resulting Cooperative Cybersecurity Initiative takes important steps by seeking three voluntary stakeholder commitments to help secure networks: (1) the adoption of an Internet Service Provider Code of Conduct to combat botnets; (2) the implementation of DNSSEC to secure the Domain Name System; and (3) the development and implementation of standards-based secure Internet routing protocols in order to prevent Internet route hijacking.

Juniper Networks believes that seeking such voluntary commitments on such an important issue is a laudable goal. We also believe a phased but accelerated approach is a sensible way to attain the level of adoption and implementation throughout industry that will be required to meet this goal. Thank you for seeking our views on this important initiative. Should you have any questions regarding this submission, please feel free to contact Mr. Robert Dix, Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks, at 571-203-2687 or rdix@juniper.net .

Sincerely,

Mitchell L. Gaynor
Executive Vice President, General Counsel and Secretary

JUNIPER NETWORKS
1194 North Mathilda Ave.
Sunnyvale, CA 94089
o +1 408 745 2000
f +1 408 745 2100
www.juniper.net

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

March 6, 2012

Mr. Larry Clinton
President and CEO
Internet Security Alliance
2500 Wilson Boulevard, Suite 245
Arlington, VA 22201

Dear Mr. Clinton,

Thank you for appearing before the Subcommittee on Communications and Technology on February 8, 2012, to testify at the hearing entitled "Cybersecurity: Threats to Communications Networks and Private-Sector Responses."

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

To facilitate the printing of the hearing record, please e-mail your responses in Word or PDF format, to katie.novaria@mail.house.gov by the close of business on Tuesday, March 20, 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

The Honorable Greg Walden

1. Mr. Lewis mentioned in his written testimony that the government could play a coordinating and incentivizing role regarding the widespread adoption of Security Extensions for the Domain Name System, also known as DNSSEC. Do you agree, and if so, what should the government do specifically?

>The government should fully deploy DNSSEC across all of its networks, including the classified and private networks that do not interconnect with the Internet, but use DNS software. Once all of the government's public-facing sites are DNSSEC-compliant, it will incentivize the ISPs, hardware, and software manufacturers to move quickly to get DNSSEC deployed across the private sector.

2. In your testimony, you mentioned the formation of an "underwriters' laboratory" style information clearinghouse for cybersecurity. Would sharing additional information with cybersecurity insurance providers, perhaps through private-sector clearinghouses and with appropriate privacy safeguards, help foster the development of such a program?

>The ISA suggestion to create an Underwriters' Laboratory for cyber security was not confined to information sharing.

The ISA has proposed an alternative model to regulation to spur greater investment by the private sector in cyber security ---not just information sharing. This alternative model is known as the "Cyber Security Social Contract." It is modeled on the "Social Contract" that private industry and the government arrived at, at the beginning of the 20th century to spur investment in the hot technologies of the time: telephones and electric power. At that point in time, there was a similar situation to cyber security today. As is the case now with cyber security, at that time, new infrastructures were being deployed, but in a limited fashion generally to high density and affluent areas. Public policy makers recognized that we needed universal deployment of electricity and telephones for the public interest, just as we need broader adoption of cyber security best practices standards and technologies today.

The policy makers of that time recognized that infrastructure enhancement is best accomplished via providing market incentives and hence they arrived at a "Social "Contract with their private owner and operator contemporaries. In that particular case, the social contract "deal" was for the public sector to guarantee the return on investment in exchange for the owners and operators deployment of their telephone and electric infrastructures to areas that were not commercially viable. That's how the public utility model was born, and it was successful.

ISA has advocated a new social contract---with different terms----for cyber security. In the current situation, private sector entities may need to be asked to deploy cyber defenses that go beyond their own commercial interests to fulfill the broader national interest, much as was the case with electric and telephone service. In this particular case, we will need to find market incentives that do not cost the federal government significant expenditure. We have advocated greater use of liability adjustments and reform, private insurance, streamlined regulation to eliminate outdated and redundant regulations, procurement advantaging, streamlined permitting, etc. This is essentially the approach that was recommended by the House Task Force on Cyber Security earlier in 2011.

In order to make this menu of incentives viable, however, there will need to be an independent entity that will assess the various standards, practices and technologies available in the marketplace for their quality. Adoption of higher value practices (usually more costly) would earn greater incentives. That entity is what we were referring to with respect to an "Underwriters' Lab"

ISA has also proposed steps that ought to be undertaken specific to stimulating the cyber insurance industry in the interests of broader national security;
We believe that the insurance industry may have a positive role to play here. To the extent that companies must report losses to their insurance carrier, who will take into consideration such losses when establishing future premium

levels, the existence of a robust insurance industry will provide market place incentives for companies to provide information about security breaches, losses and investments, as well as provide incentives to take action to reduce such breaches, losses and investments.

Moreover, existing information sharing mechanisms can be and should be improved. The lack of antitrust exemptions still creates a chilling impact on information sharing. Additionally, even assuming no antitrust issues, there is insufficient motivation for the insurance industry to share rate and loss information. Such sharing of information within the insurance industry could provide substantial benefits as it does today arising from such brick-and-mortar organizations, such as, the Insurance Service Organization (ISO) and Underwriter's Laboratory (UL).

In addition, providing R&D funds to a potential insurance information sharing organization for the study of frequency and severity of losses could prompt more insurers to provide cyber insurance as well as create de facto best practices and agreed upon loss statistics.

There can be no doubt that a broader deployment of cyber insurance not only allows a mechanism for promoting good practices, but also provides a private sector funded mechanism for assessing compliance. When insurance companies have their own money on the line, they have an enormous economic incentive to assure that the practices they are insuring are in fact being followed, which has the concomitant societal advantage of further assuring better cyber security.

Cyber insurance can improve overall cyber security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cybersecurity.

The security requirements used by cyber insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber losses, they have a strong interest in greater security, and their requirements are continually increasing.

As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses to return to normal and reducing the need for government assistance.

Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding.

Despite the benefits of cyber-insurance, the market for cyber-insurance is adversely affected by a number of problems.

First and foremost, insurers are afraid of potential claim volumes. Cyber-hurricanes represent an uncertain risk of very large losses, and, as such, are very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability. In addition, "cyber-hurricanes" raise a barrier to entry to the insurance market, because an insurer may be wiped out if a major event occurs before they have built up sufficient cash reserves

Prices for private market reinsurance for cyber-insurers are extremely high as the fear of a hurricane" is felt most by the reinsurance community.

In essence, cyber insurance is a relatively new area, and, thus, insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing the price of policies, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether to purchase insurance against a particular risk.

3. Several members of the panel highlighted the need to remove legal impediments that may prevent Internet service providers, cybersecurity software providers, and others to address cyber threats and share information. Could you identify any specific federal or state laws, regulations, or other legal impediments that Congress can address to improve cybersecurity?

>Current Federal law potentially restricted the use of certain communications information to protect end-users in some circumstances and the voluntary sharing of communications-related information with governmental entities (outside of limited exigent circumstances). Moreover, the laws of some States are arguably even more restrictive than current federal law in this area.
Against this regulatory back-drop, owners and operators of Internet networks have at times agreed to a range of contractual or other voluntary restrictions (in privacy policies, for example) on information collection, use, and disclosure that have the effect of limiting their ability to collect and share communications-related information with third parties and the government.

Many of these legal and contractual restrictions were created to protect privacy and to impose checks on law enforcement access to private citizens' communications. These are important public policy goals, but the rules that exist today were largely crafted in the context of the telephone network, and certainly well before development and widespread use of many of today's Internet-based communications technologies.

For example, many current laws, particularly at the state level, speak in terms of "eavesdropping" on "private conversations" and to "all party" consent, terms that may be hard to apply in the context of Internet-based communications that may transmit voice as data (e.g., VoIP) or contain multiple layers of "communication" (client server communications as well as embedded user-generated content). Thus, the current state of the law creates some uncertainty with respect to whether the use of certain types of Internet-based communications information is authorized for certain purposes. When coupled with potential criminal liability and civil causes of action under almost all such federal and state laws, this existing legal framework deters some beneficial service provider activity in the area of cyber security and thwarts information sharing. Pending Congressional legislation provides an opportunity and a vehicle through which to provide greater clarity in this area by establishing a common set of rules for the Internet in this regard.

Accordingly, legislation should be updated and changes made to provide enhanced clarity around the use of communications-management technologies to enable greater levels of security and protection from a wider range of malicious online activity than was ever possible or necessary in the legacy telephone networks.

While existing law already allows providers to collect, use, and disclose communications information for certain purposes, Federal legislation could provide greater clarity around a provider's right to collect, use, and disclose communications information for cyber security purposes. And although existing law allows providers to share information with the government in certain circumstances, such circumstances should be expanded to include those in which the government is a customer and the information in question relates to the cyber security of the government's systems, and where the information is being made available to the government through an appropriate cyber security information clearinghouse. Finally, in order to address cost issues and harness the power of market-based incentives for investment in cyber security at all levels of the technology development process (from Silicon Valley, to Wall Street, to provider networks across the country), providers should be

authorized to collect, use, and disclose communications-related information as part of the provision of any service (security or otherwise) that a subscriber has affirmatively requested to receive. Such a change would allow providers—with the affirmative, opt-in consent of a customer—to use that customer's communications information to provide services requested by that customer, and, thus, would provide a means of delivering advanced cyber security services to customers and of funding the development and deployment of robust technologies that may be used in furtherance of cybersecurity initiatives and activities.

Some suggested changes to specific Federal laws that will help implement greater information sharing are set forth below:

> Authorization for Information Collection, Use and Disclosure in Connection with Cybersecurity Activities.
> Section 2511(2)(a) of chapter 119, title 18, United States
> Code, is amended—
>
> (1) by adding a new subsection (iv) as follows;
>
> (iv) It shall not be unlawful under this title [18 USCS §§ 1 et seq.] or under any other federal, state, local, or other law4, and no civil action or criminal charge may be brought in any court5, where a wire or electronic communication service provider or a remote computing service provider[1], including any director, officer, employee, or agent thereof, whose facilities are used in the transmission, processing, or storage of a wire or electronic communication, intercepts, discloses, or uses that communication while engaged in any activity relating to[2] the cybersecurity of its networks, operations or users, the provision of any service relating to cybersecurity, or any activity for which the provider has obtained affirmative, opt-in consent[3] of the customer or subscriber to whose service such communication relates.[4]

---

[1] This provider reference references two relevant types of service providers under existing Federal law regulating access to electronic communications: "electronic communication service" is defined in 18 U.S.C. § 2510(15) and "remote computing service" is defined in 18 U.S.C. § 2711(2). Electronic communication service providers and remote computing service providers may each require the flexibility to use communications information as outlined in certain situations.

[2] Under current Federal law, there are two different standards governing when electronic communication service providers may use communications-related information for security purposes: (1) Under 18 U.S.C. § 2511(2)(a)(i), activity that involves communications "content" must be "a necessary incident to" the protection of the provider's rights or property (this has been narrowly construed by some courts, and may not extend to protection of users in all cases), and (2) whereas an electronic communication service provider may use "non-content" information such as traffic data—to/from IP addresses, dates/times, etc.—for activities "relating to" not only the protection of its own rights or property, but the protection of any user of that service from fraudulent, unlawful or abusive use of service as well. *See*, 18 U.S.C. § 2511(h) and 18 U.S.C. § 3121(b)(1)-(2). The above amendment proposes adoption of the "relating to" standard in connection with cyber security activities, and application of that standard to uses of not only "non-content" information, such as, traffic data, but, because concepts of content and non-content are blurred in the context of the layered structure of information in an Internet communication packet, the full "contents" of the communications as well.

[3] By including this provision, this will preempt any state law that purports to require "two party" or "all party" consent to recording or use of communications. However, to balance privacy rights, this phrase suggests that such use must be with affirmative opt-in consent, to avoid situations where customers find themselves ensnared by services offered on an opt-out basis. This parallels existing frameworks regulating the use and disclosure of sensitive personal information, ranging from financial information to health information to communications-related information where service providers are authorized to use and disclose customer information with that customer's consent.

Authorization for Disclosure of Information to Governmental Entities. Section 2702 of chapter 121, title 18, United States Code, is hereby amended—

(1) by adding to subsection (b) a new subsection (9) as follows;

(9) to a governmental entity if the governmental entity is a customer of the provider and the information in question relates to the cybersecurity of the governmental entity's information systems and networks or if the information is being made available to any governmental entity through an appropriate cyber security threat and vulnerability information clearinghouse.

(2) by adding to subsection (c) a new subsection (7) as follows;

(7) to a governmental entity if the governmental entity is a customer of the provider and the information in question relates to the cyber security of the governmental entity's information systems and networks or if the information is being made available to any governmental entity through an appropriate cyber security threat and vulnerability information clearinghouse.[5]

4. I have seen reports that indicate that many cybersecurity breaches could be avoided if businesses followed best practices. What are some of these techniques and how can we encourage more companies to adopt them?

> Please see the attached Data Breach Investigations Report jointly conducted by the US Secret Service and Verizon. Best practices start on page 65. This document provides an excellent starting point for proven cyber security best practices.

However, the problem in cyber security is not the absence of effective standards and practices, but getting the practices to be implemented. While it is often noted that businesses should adopt good security practices to protect their systems several, independent studies from entities such as PricewaterhouseCoopers and the Center for Strategic and International Studies/McAfee have documented that cost is the primary barrier to adopting adequate cyber security standards and practices.

---

[4] Many service providers link communications activity to IP addresses. Providers do not know, however, whose fingers are actually on the keyboard. Nevertheless, certain federal and/or state laws require that the consent obtained be from the actual user, not just the subscriber or customer. To address this issue, the phrasing above is suggested to clarify that the operative consent for providing services requested by a customer is the consent of the customer or subscriber, not necessarily the consent of each and every individual user that the customer allows to use their service. This approach is consistent with the way consent is administered for many communications services today including caller ID, which when originally introduced, potentially violated laws in some states regulating use of trap-and-trace devices (devices that identify the calling number).

[5] Issues of service provider liability under conflicting state laws and private contracts with respect to disclosures to government under these two new authorizations should be able to be cared for within the existing statutory framework in chapter 121, title 18. Specifically, potential liability under state laws or private contracts can likely be addressed under existing language in 18 U.S.C. §§ 2703(e) and 2707(e)(1). In order to do so, however, it would be desirable for the legislative history of the bill that enacts these changes to provide that it is the intent of Congress that these existing provisions should serve to preempt conflicting state laws and immunize providers from any claims arising out of the provision of information to the government under the new statutory authorizations proposed for 18 U.S.C. § 2702, above.

Of course there is considerable investment by the private sector in cyber security. According to the Ponemon Institute/Bloomberg Report released in January 2012, private sector investment in cyber security has nearly doubled in the last five years from approximately $40 billion to $80 billion. However, the investment is uneven. Large sophisticated entities are investing significantly. However, on the other side, there are a large number of companies that have actually leveled off or even reduced their investment in cyber security in the last 3 years--- largely due to the poor economy.

It also needs to be understood that there are substantial economic incentives for enterprises to become less secure. Many modern platforms, such as, VoIP and cloud computing are substantially less secure than previous platforms. Entities adopt these new platforms, however, because of their tremendous cost savings.

Finally, there is the core problem that defines cyber security, which is the interconnection problem. An entity can do all that it ought to, to secure itself, but if it is interconnected with other systems that do not practice adequate security, it too will be less secure. In an age characterized by extended partnerships and supply chains that can be hundreds or thousands of companies long, this interconnection issue can be extremely problematic.

That is why the a series of reports, including the ISA Cyber Security Supply Chain Project, the White House's "Cyberspace Policy Review," the pan-industry/civil liberties white paper (signed on to by the Chamber of Commerce, the Business Software Alliance, TechAmerica, the Center for Democracy and Technology and the ISA) as well as the House Cyber Security Task Force have all recommended that government develop a menu of market incentives to drive greater adoption of sound security best practices and standards.

5. The Internet is currently transitioning from IPv4 to IPv6 addressing. Does that process create any new cybersecurity issues? Will transitioning to IPv6 alone solve any cybersecurity issues that currently exist? Does the process of transitioning to IPv6 present opportunities to resolve existing cybersecurity issues?

> The transition to IPv6 is only to provide an increase in unique addresses for Internet devices. While some security features are added (such as mandatory IPSec), those features are already optional in IPv4. The only security issue that gets "solved" by IPv6 if used according to its original intent is attribution of packet sources and destinations. But that comes at the loss of anonymity, something that has been very powerful in both the growth of the Internet as well as an unintended level of security (via obscurity generated by IPv4 address translation technologies.) IPv6 will have a minimal technical impact on the current cyber security problems. The vast majority of today's problems are with applications, software, websites, email, and user actions. IPv6 will bring new security issues that won't be visible until we have wide-spread adoption of the protocol.

6. In December, we heard from witnesses that the implementation of "WhoIs" databases makes it difficult for companies and law enforcement to identify and track down the owners of websites that are facilitating illegal conduct, including sites that host malware. What is the private sector doing to strengthen the use of WhoIs to help combat cybercriminals, and are there any steps Congress can take to facilitate that work?

> Rules for operating WhoIs services are set by the ICANN, and allow for anonymous registration of domain names. That's a two-edged sword, and something best left unfettered by the Congress.

7. You mentioned in your written testimony that the Internet Security Alliance has worked to secure telecommunications supply chains. Could you explain what steps the private sector is taking in this space and whether you see a role for the federal government to facilitate supply chain security?

The ISA will shortly publish a 60-page program for securing the IT Supply Chain, which includes specific recommendations for actions that government can take to support this effort (see chapter 9 of the attached)

As with other areas of cyber security, the key notion is to make security affordable. As a result, the ISA supply chain program is not based on independently derived sets of standards that can be "bolted on" to normal business practices, but rather developing management and business practices wherein good cyber security is "built in."

The attached ISA Supply Chain Programmatic document is based on a 4 year effort that involved scores of corporations, a half-dozen federal agencies, as well as research institutions. The key driver in the development of the ISA program is that the procedures must be cost effective.

The Honorable Anna Eshoo

Several agencies, including the FCC have been exploring a voluntary, industry "code of conduct" as a way to address the detection and mitigation of botnets. Do you support such an effort and how do we ensure it's effective?

> The FCC's CSRIC is working on a voluntary code for ISPs, which is expected to be finished later this month. We support any effort where ISPs and others in the Internet community are working together to develop and promote best practices. However, we need to extend this effort beyond the ISPs, since most of the "root cause" of botnets lies in software vulnerabilities, improper user actions, and lack of law enforcement's ability to track down and prosecute the criminal groups behind them. ISPs are only a part of cyberspace, and cannot be seen as the only place where security steps can be taken.

The Honorable Henry Waxman

1. The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) has been formulating recommendations for best practices to ensure optimal security and reliability of communications systems. How do you see this process contributing to improvements in cybersecurity?

> see the answer above.

2. What opportunities do you envision for government and industry to work together towards coming up with critical cybersecurity solutions? What role specifically do you see for the FCC?

> Government and industry are "peers" in cyberspace, in that they both operate and manage different parts of cyberspace that interact with each other at millisecond speeds. Rather than focusing on a traditional role of government in forming laws and regulations, it would be more helpful if government functioned as a peer with the private sector, working together to solve these problems. We need the government to be as secure, or even more secure, than the private sector.

The current role of the FCC in cyber security (fostering collaborative development of industry best practices) is appropriate. It would be impossible for the FCC to "regulate" the security of the Internet in a manner similar to how they regulate spectrum usage, licensing of radio and TV stations, and similar communications functions. Cyberspace is vastly different from the electromagnetic spectrum and requires a very different approach in terms of its management and operations.

THE ISA GUIDELINES FOR SECURING THE ELECTRONICS SUPPLY CHAIN
(DRAFT VERSION FOR COMMENT)

By Scott Borg

Contents

General Principles	2
1. The Product Design Phase	9
2. The Photomask Production Phase	16
3. The Microelectronic Fabrication Phase	21
4. The Circuit Board Fabrication Phase	28
5. The Board Pre-Assembly Phase	33
6. The Product Assembly Phase	39
7. The Product Distribution Phase	47
8. The Product Maintenance and Disposal Phase	48
9. The Necessary Legal Conditions	53
Expert Contributors to This Project	57

© 2012 Internet Security Alliance

General Principles

The purpose of these guidelines

- These guidelines are instructions for securing the global electronics supply chain. They describe the security procedures that need to be implemented at each of the various stages in the production of electronics products. This systematic effort to secure the electronics supply chain has become necessary, because electronics manufacturing is now a series of intricately connected processes that need to be distributed across many different countries and regions in order to maximize quality while minimizing cost.
- The primarily purpose of these guidelines is to protect global electronics companies from major economic losses.

  The sorts of losses that need to be prevented include:
  I) losses due to interruptions or delays in production, including those due to false or misleading reports on production start dates, available capacity, production rates, quality test results, inventories, and delivery dates;
  II) losses due to diversions or corruptions of production, including the outright theft of parts and products, insider sabotage, the counterfeiting of electronic products, and the substitution of inferior components;
  III) losses due to the discrediting of processes or products, including uncertainties about quality, concern about product support, and adverse publicity involving the treatment of workers, environmental impact, and business affiliations;
  IV) losses due to the theft of competitively important information, including diffuse, but competitively important business and production information, as well as recognized intellectual properties.

  The enormous scale of the losses that global electronics companies have suffered due to these security problems in their supply chains means that there is now an enormous incentive to implement guidelines of this kind.

  These guidelines are *not* intended to burden electronics manufacturers with more costs. The security measures included in them are intended to pay for themselves many times over by reducing losses. Collectively, these security measures should ultimately deliver considerable increased profits by allowing the implementation of more efficient and advanced global manufacturing.
- In addition to benefiting global electronics companies, these guidelines are designed to help existing electronics suppliers claim credit for their security achievements and protect their own interests better. Explicitly identifying the security procedures that electronics suppliers are expected to follow should provide a competitive advantage to the companies that are doing a good job of implementing these procedures. Meanwhile, these security guidelines should help electronic suppliers protect themselves from physical thefts, damage to reputation, loss of intellectual property, and many of the other types of damages that global electronics companies also need to avoid.
- These guidelines should help, not just existing electronics companies, but also companies and countries that wish to become electronics suppliers. This is because the guidelines spell out exactly what will be required of new entrants to the electronics markets as far as security is concerned. Once companies and countries know these requirements, it becomes much easier for them to satisfy the security concerns of their potential corporate customers. In addition to providing those companies and countries with new opportunities for economic

© 2012 Internet Security Alliance

development, the result should ultimately be a more geographically diverse and, hence, more resilient electronics supply chain.

- These guidelines should therefore be used as a reference document in the drafting of contracts between the producers of electronics products and their suppliers. They should be applied in a way that coordinates security throughout the electronics supply chain and that provides a common standard that competing bidders should be expected to meet. Establishing a common set of expectations about what security measures will be specified in electronics supply contracts should also greatly reduce the time and costs of negotiating those contracts.
- Governments will have ample reason to support the adoption of these guidelines. This is because implementing these guidelines will make it enormously more difficult to insert malicious firmware or defective components into electronic products destined for use by military forces or critical infrastructure industries. Since most direct programs to secure electronics manufacturing for government and military use have little hope of being economically viable, the best hope governments have of securing their electronic systems is to make this effect a by-product of a security program instituted entirely for other business reasons.
- These guidelines should help the electronics industry to secure even more of the benefits of sensible globalization. If electronics manufacturing utilizes sufficiently effective security measures, and if there is sufficient reason to believe that these security measures are being carried out in good faith, then it ideally shouldn't matter who carries out any manufacturing phase, where that manufacturing phase is being carried out, or who owns the facility that is being used for it.
- The overall result of these guidelines should be a more efficient, fairer, and more resilient electronics supply chain, with lower risks for every participant.

The general principles for applying these guidelines

- The point of these guidelines is to deliver technical and economic results, not put companies through more administrative formalities. Hence, these guidelines describe the actual, operational procedures that need to be carried out, not the administrative arrangements or policy declarations that might be necessary to implement these operational procedures.
- These guidelines are shaped as much by economic considerations as by technological considerations. Every security measure needs to have a cost that is significantly less than the probable loss of value that the security measure is preventing. In other words, every security measure needs to be cost-effective. If any "best practice" is really the best practice from a business or economic standpoint, it should be made a standard practice.
- Many of these guidelines do not describe security measures as such, but instead describe ways of carrying out manufacturing operations. This is because the most cost-effective way to deal with many security issues is not to add extra protective measures, but to arrange the way business is done so that extra protective measures become unnecessary or, at least, much cheaper.
- It should always be made legally and contractually possible to dispense with any given security measure if a more effective measure is substituted instead, but the producer of the final product will need to acknowledge that the security measure being substituted is indeed more effective.

© 2012 Internet Security Alliance

- The corporate customer that is responsible for the final product may wish to excuse some suppliers from carrying out some of these security measures if those security measures are not important for a particular and if dropping those security measures would significantly reduce the suppliers' costs. A consumer product that has no chance of being used in a critical application, for example, does not need to be as carefully protected from the insertion of counterfeit parts and malicious firmware. Similarly, a product that is truly generic and contains no distinctive intellectual property does not need to have its design features protected from intellectual property theft.

  However, care should be taken in relaxing the security in facilities that will need to be secure for the production of other products. Many of these security measures, once instituted, cost very little to keep in place. Relaxing these security measures part of the time and then tightening them the rest of the time may actually increase costs. Once security measures have been temporarily relaxed, it may become much more difficult to persuade employees to maintain them in the future. Altogether, attempting to save money by selectively or temporarily relaxing these security measures may turn out to be a poor economy for all concerned.

- The security measures marked here with an asterisk* are greatly needed and potentially cost-effective, but currently difficult to carry out, because the necessary tools and services are not yet readily commercially available. Hence, while serious consideration should be given to instituting these security measures, doing so may not yet be cost-effective for many manufacturers.

- An effort has been made throughout this document to adjust the language so that the guidelines will be comprehensible to those who are not technical specialists, who come from different parts of the industry, or who have different linguistic backgrounds. It is hoped that the resulting use of fresh language to describe many security procedures will also cause security professionals to stop and think about what is really involved in each security measure.

The supply chain phases used to organize these guidelines

- The successive phases, into which these guidelines are organized, represent the stages nearly every electronic product goes through. They start with the products conception and then run through (1) the design process, (2) the production of the photomasks to be used in the manufacture of the microelectronic components, (3) the actual manufacture of those micro-electronic components, (4) the manufacture of the printed circuit boards used to connect and hold the other electronic components, (5) the "pre-assembly" of those components into loaded circuit boards, (6) the assembly of the actual electronic products, (7) their distribution though intermediary steps to end-users, and (8) the maintenance they receive during their usage life, ending with their disposal.

- All these phases of the electronic supply chain are remarkably the same whether the electronic product is a laptop computer, a server, an airplane, a smart phone, a router, a gaming console, or a credit card reader.

- In addition to covering each stage in the manufacturing process, these guidelines include a section (9) on the legal conditions that need to be in place for the rest of the guidelines to be implemented effectively. Some of these legal conditions can be put in place by the corporations involved, but others need the legislative and governmental support of the countries endeavoring to gain or maintain a competitive position in the global markets for electronics manufacturing.

© 2012 Internet Security Alliance

- The guidelines for each phase of the electronics supply chain are designed to be complete and self-contained. Hence, only one section of the guidelines will need to be applied to any given phase of production. Accomplishing this required a modest amount of repetition, but there was no good way to avoid this, because hardly any of the repeated guidelines were repeated throughout every phase of production.
- The complete guidelines outlined in this document may seem lengthy, but the guidelines for securing any single phase of the electronics production process are not. The complete set of guidelines needed to be conceived and developed together, because the security measures instituted in one phase of the electronics supply can have a profound effect on the security measures that are needed in other phases. When it comes to implementing these guidelines, however, they can generally be treated as nine separate sets of guidelines. This means that the number of guidelines that will need to be incorporated into any given supply contract is actually not very large.

The process by which the guidelines were produced

- These guidelines are all based on recommendations and anecdotes from people with extensive field experience. Nearly every guideline included here is currently the normal practice of some global electronics company in some portion of its operations. Most of these practices were instituted in response to actual security problems that have resulted in considerable losses or could have resulted in considerable losses. Although the people responsible for these security practices were able to describe them in detail, many of these practices do not seem to have been previously codified or made into written policy.
- The original basis for these guidelines was an extensive series of conferences, workshops, and meetings organized and sponsored by the Internet Security Alliance over a period of roughly four years. The participants in these events included representatives from forty-six corporations, six government departments or agencies, five research institutions, a law firm, and two trade associations. The individuals involved are listed at the end of this document, except for a small number who wished to remain anonymous. The main results of these conferences, workshops, and meetings were long lists of security problems, numerous anecdotes about particular security cases, and a large collection of comments about relative security priorities and points that deserve special attention.
- Based on these results, Scott Borg carried out large numbers of interviews with individual experts who had dealt in field situations with the specific security issues that had been identified. These experts provided step-by-step descriptions of the individual operations that needed to be secured, the security measures that needed to be taken to secure those operations, and other measures that had been tried, but abandoned as ineffective or too expensive for what they accomplished. The individuals and companies involved were extraordinarily generous in sharing their best practices. It is these actual practices that provided the material for these guidelines.
- The drafts of individual guidelines were all based these interviews with individual experts, along with periodic reviews of the conference and workshop records. In many cases, there were multiple interviews addressing the same point, which then had to be collated, studied, and evaluated. The drafting of each individual guideline was thus the outcome of a fairly elaborate process, even before the various drafts were sent back to the contributing experts for review.
- All of the actual guidelines were drafted by Scott Borg, except for about twenty legal guidelines that were drafted by Nick Akerman. No guidelines were drafted by anyone else. The drafts of the guidelines were circulated extensively for comments among the workshop

© 2012 Internet Security Alliance

participants and among the specialists in each facet of electronics supply chain security. As the comments were collected, the drafts were repeatedly revised and re-circulated until virtually all of the best qualified security experts for each phase of the electronics manufacturing process were satisfied with them.

The efforts to make sure these guidelines are cost-effective

- Every guideline that was considered for inclusion in this document was examined carefully from the standpoint of cost-effectiveness. This resulted in many familiar security measures being deliberately omitted, at least for certain phases of the supply chain. It also resulted in some relatively unfamiliar security measures being included. Some of the security procedures that had previously been standard practice were intentionally dropped, because the experts who contributed to the writing of these guidelines could not come up with any good reason why those procedures should be considered cost-effective. Meanwhile, other security measures that might sound odd or "excessively fussy" to those whose knowledge of the subject is largely theoretical have been included, because they were found in practice to be efficient ways of dealing with important real-life security problems.
- The stringency of the security measures and the degree of detail in the guidelines has been carefully adjusted to fit the probable level of risk in each operation and at each stage of the supply chain. Thus, for example, the security guidelines for the design phase are much more elaborate than the security guidelines for the circuit board pre-assembly phase. This is because the harm that could be caused by insufficient security in the design phase is much greater than the harm that could be caused by insufficient security in the circuit board pre-assembly phase.
- The emphasis here is not on doing as many things as possible to secure each phase of the manufacturing supply chain, but on doing the right things. Some readers of these guidelines will probably find that the security measures that have been included suggest additional measures that have been left out. In most cases, these omissions are deliberate. The additional security measures, which seem like obvious steps to take, were reveled on closer examination to be ineffective or superfluous, given the other measures and systems in place. The few exceptions, where measures of limited effectivenes were retained in these guidelines, are generally cases where the measures in question serve legal purposes, laying the ground for possible legal actions.
- A special effort was made to avoid mechanically repeating the same security measures in different production phases. Often when people drafting standards and guidelines have identified a useful security measure, they assume that it should be applied everywhere. But the same security measures have very different costs and yield very different benefits in different phases of the supply chain. Repeating a security measure that is vital at an early stage in the supply chain may be a complete waste of resources at a later stage in the supply chain.
- Some guidelines are included here that would not have been cost-effective as recently as two or three years ago, but have now become cost-effective, due to the falling costs of data storage and electronic equipment. It is now practical, for example, to record and store large quantities of access logs and high-quality surveillance videos that would have been too expensive to keep only a few years ago.
- Most of the security measures that have been included in these guidelines are remarkably inexpensive if they are built into the architecture and operating procedures of the various production phases when the operations and facilities are being laid out or when they are being structurally renovated. These security measures will only seem burdensome if,

© 2012 Internet Security Alliance

instead of being integrated into the operational planning, they are tacked on later as a kind of afterthought.

- Because many of these security measures need to be built into the architecture and operating procedures of the various production facilities, it is recommended that the companies that will be expected to carry out the security measures be allowed a reasonable period of time to phase them in. However, it would be reasonable to give preference in the awarding of supply contracts to those companies that are already carrying out these security procedures or that will be able institute them sooner.
- Because several of the factors that determine the cost-effectiveness of security measures are changing over time, the cost-effectiveness on each security measure will need to be regularly re-evaluated.

The need to understand the guidelines' collective functions

- Many of the individual guidelines have a beneficial effect on security only when used in conjunction with other guidelines. Hence, care should be taken in relaxing any one of these guidelines or substituting a different security measure, because several other guidelines may be affected.
- Many of the individual guidelines are accomplishing several things at the same time. Hence, if one effect of the guideline becomes less important, other effects may remain as important as ever.
- There is no substitute for a sincere and thoughtful effort to provide good security. This effort needs to be informed by a wider vision of the factors that collectively determine risk, including the changing nature of the threats, the possible consequences of various security lapses, and the new methods under development for reducing vulnerabilities.
- The wider vision that provides a context for the application of these guidelines and the theoretical concepts that underlie them are beyond the scope of this current document. They can be found in other literature, including "Securing the Supply Chain for Electronic Equipment: A Strategy and Framework" (2009) and *Cyber Vulnerability Analysis* (forthcoming), in which the author of these guidelines discusses the theory and rationale behind them.
- To be genuinely effective, these guidelines will need to be applied, not mechanically, but in good faith and with understanding.

The relationship of these guidelines to other check lists, standards, and guidelines

- These guidelines were drafted entirely from scratch, without reference to any other check lists, standards, or guidelines. This is because there had previously been no comprehensive attempt to describe the practices necessary for securing electronics manufacturing. There have been check lists and guidelines aimed at securing many related things, including: corporate and government information systems, software products, software development processes, computer networks, and telecommunications systems. But the secure manufacturing of electronic equipment, on which most of these other things rely, has not been previously tackled in any thorough or systematic way. The fact that this was a pioneering effort made it easy to take a fresh look at the subject, but it also made the work progress more slowly than it might otherwise have done.
- These guidelines are not intended to replace guidelines and standards that describe general cyber security measures, but should be used in conjunction with those. The current

© 2012 Internet Security Alliance

guidelines describe how to limit the types and extent of the information systems deployed in electronics manufacturing facilities. They also describe some special cyber security measures that need to be implemented in the certain parts of the electronics manufacturing process. But any information systems employed by electronics manufacturers will still need to be secured in standard ways, and other, more general cyber-security guidelines will be helpful with that.

- These guidelines are also not intended to replace guidelines and standards that focus more narrowly on the cyber security of automated industrial control systems. Securing automated controls is an important part of a layered defense strategy for manufacturing facilities. Hence, the special security measures that can be taken to reduce the vulnerabilities of programmable logic controllers (PLC's), distributed control systems (DCS's), and other automated controls should be implemented wherever possible in electronics manufacturing facilities.
- The guidelines and standards that these current guidelines *are* intended to replace, as least where electronics manufacturing is concerned, are guideline that were not designed specifically for the electronics supply chain, but have been used for that kind of supply chain in the past, because nothing more appropriate was available. These other types of guidelines include guidelines originally intended to provide security for general manufacturing, for other types of supply chains, and for software development. Guidelines of these kinds may be useful in securing operations that are complementary to electronics manufacturing, but they are not sufficient or even appropriate for securing the manufacturing of the electronics hardware itself.
- During the more than four years in which these guidelines have been under development, a number of other efforts concerned with the security of electronics manufacturing have gotten underway. The people involved in these other efforts were invited to the ISA workshops, and several of them became regular participants. The people involved in the other efforts were also provided with the reports, preliminary findings, and earlier guideline drafts that emerged from the ISA-sponsored effort. Meanwhile, a number of electronics manufacturers had begun to codify their security procedures. As they did this, they were encouraged to draw on the findings of the ISA workshops and to offer suggestions for the guideline drafts as these were being developed. As a result, there has been considerable informal coordination between these efforts, and the information and insights embodied in these guidelines have already been very influential.
- One of the useful complementary documents produced by participants in the ISA electronics supply chain workshops is *NISTIR (Draft) 7622: Piloting Supply Chain Risk Management Practices for Federal Information Systems* (2010), by Marianne Swanson, Nadya Bartol, and Rama Moorthy. This provides an overview of some relevant administrative and policy requirements, as well as highlighting some security measures that are of special importance.
- Because these guidelines focus on the concrete security measures that need to be implemented, rather than on the procedures and policies necessary for implementing them, organizations employing these guidelines may wish to supplement them with other guidelines or standards that focus on administrative procedures. One of the most useful and best known of these other standards and guidelines is the *ISO 27001*, which focuses on the management procedures for information security systems.

© 2012 Internet Security Alliance

1. The Product Design Phase

General product design

Procedural policies to be followed throughout the design process

1.001 Initiate the planning and tracking of security provisions at the very beginning of the design process, so that they become part of the work procedures for each step.

1.002 Limit the personnel with access to the design facilities to those who genuinely need to be there.

1.003 Document the arrivals and departures of all personnel entering the design facilities.

1.004 Use two or three factor authentication (e.g., photo RFID and fingerprint) for all personnel entering and leaving the design facilities, unless the design team is small enough so that the relevant security staff and the members of the design team all know each other.

1.005 Make sure design meetings are held in rooms that do not adjoin public areas or have public-facing windows.

1.006 Scan everyone entering or leaving the design facilities for devices that could be used to capture or transport large quantities of information, such as personal laptops, flash drives, iPods, digital cameras, CD burners, and CD's.

1.007 Do not allow cell phones, especially smart phones, to be brought into any important design meetings (because they can be remotely accessed and turned into listening devices).

1.008 Make sure the networks used in the design process are completely isolated from the other corporate networks.

1.009 Require two-factor authentication for any access to the computers used in the design process.

1.010 Set the access controls in the design facility's information systems so that they only allow an employee to access the systems and documents deemed necessary for that employee's work assignment.

1.011 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

1.012 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

1.013 Maintain regular logs recording which personnel access which design documents or data and at what times.

1.014 Arrange for any abnormally large downloads of design information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

1.015 Record which parts of the design documents each person generates, writes, or revises.

1.016 Make sure any transmission of designs or data relevant to the designs is strongly encrypted if it is being sent to an outside partner or to a different physical facility.

1.017 Make sure the computers and other equipment used in the design process cannot be physically accessed by outside personnel, such as cleaning staffs.

© 2012 Internet Security Alliance

1.018 If cleaning staff or other maintenance personnel need to be admitted into rooms where equipment containing sensitive design information is stored, these people should either be given the same sort of background check as the design personnel or else be personally escorted by a trusted member of the design team, as well as having their actions video taped.

1.019 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information employed in the design process and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Personnel policies to be followed throughout the design process

1.020 Make sure all personnel who will be admitted to the design facilities are given a thorough background check, including financial identifiers and employment histories.

1.021 Require each contributor to the design process to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them.

1.022 Require each employee in the design process to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

1.023 Conduct entrance interviews in which each person joining the design team confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this design project.

1.024 Require each employee in the design process to sign an agreement specifying that he or she has not retained documents from a previous employer containing trade secrets, confidential data, or other intellectual property.

1.025 Explicitly define the limitations on the physical and digital access privileges of each employee.

1.026 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

1.027 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

1.028 Impress upon the design team the need to refrain from discussing design problems and goals in places where people outside the design team are present, such as company cafeterias and elevators.

1.029 Make sure design personnel are not given work assignments that would inevitably lead them to draw on trade secrets, confidential data, or other intellectual property from their previous employers.

1.030 Make sure that an employee's physical and digital access to the design facilities and their information systems is ended at the same time his or her work responsibilities inside those facilities are ended.

1.031 Conduct exit interviews in which anyone leaving a company involved in the design process confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that company can be used in future jobs.

© 2012 Internet Security Alliance

1.032 Warn design personnel who are leaving the company that any physical or electronic information pertaining to the design process must be securely destroyed or returned to the company, including rough notes and drawings used to jot down design ideas.

Specification of the overall physical design features and the electronic inputs and outputs

1.033 Make the designers aware that they are responsible for designing the product in such a way that it can be produced securely.

1.034 Make the designers aware that they are responsible for designing the product in such a way that the company's intellectual property cannot be easily extracted from the finished product.

1.035 Make the designers aware that they are responsible for designing the product in such a way that the product does not cause security problems for the end-users.

1.036 Make the overall physical requirements for the product restrictive enough to minimize the space available for illicit add-ons, such as wireless receivers and transmitters.

1.037 Make the product specifications *complete enough* so that covert modifications or additions would be more difficult.

1.038 Make the product specifications *narrow enough* so that covert modifications or additions would be more difficult.

1.039 Require the design staff to be trained (and given an annual refresher course) in the current techniques for hacking hardware and the ways product design needs to take account of security.

Modularization of product design

Breaking the design into modules and determining their production methods

1.040 When dividing the design into functional modules, consider where customized modules, rather than generic ones, could add robustness, as well as where they could add capabilities.

1.041 If possible, include security features in the specifications of the modular inputs and outputs.

1.042 Where possible, design "loose-couplings" between critical modules, so that privilege limitations can be introduced between modules, and so that a compromise of one module doesn't always compromise all the rest.*

1.043 Make the protection of intellectual property, as well as direct cost, a major factor in deciding which modules should be components manufactured directly, which should be components that are outsourced, and which should be components that are purchased.

1.044 Specify the electronic inputs and outputs of critical, custom-made components with enough precision to limit the latitude for deviations from the specified design.

1.045 Investigate the security, as well as the performance, of any pre-existing modular designs that are going to be purchased from outside developers.

Simulation of modular interactions

1.046 Explicitly determine the performance range that can be tolerated from each component, given the ways other components might be affected by it.

© 2012 Internet Security Alliance

1.047 Explicitly determine the relative criticality of each component, considering the difficulty and cost of replacing it, the degree to which its performance can vary without seriously undermining the product's main functions, and the extent to which its likely malfunctions could damage other components.

1.048 Explicitly determine the relative criticality of each "bus" that transfers data between components, identifying the ways in which the signals traveling through it might be improperly blocked, modified, tapped, or redirected, and assessing the consequences of those actions.

Schematic product design

Creation of schematic diagrams using circuit design software

1.049 Compartmentalize design operations to protect intellectual properties.

1.050 Turn off unneeded schematic development tool options.

1.051 Make sure each human operation in the application of the circuit design software is verified or reviewed by a second person.

1.052 Limit the privileges of those working on the circuit designs to their areas of responsibility, so that they cannot access other portions of the circuit designs.

1.053 Document each schematic design operation, including those that resulted in discarded options, noting who carried out which operation, and when they did it.

1.054 Make sure the hard disks used in the schematic design process are securely wiped and reloaded with the original design software before being used for different projects.

Testing of detailed circuit designs in simulations

1.055 Verify the validity and integrity of the simulation software.

1.056 Protect the simulation software from alteration after its validity and integrity has been verified.

1.057 Verify the validity and integrity of any patches or upgrades before these are applied to the simulation software.

1.058 Remove test features and access passwords before passing the design on.

1.059 Use the circuit simulations, not just to verify that the circuits will function as planned, but also to verify or correct the previous assessments of each component's and bus's criticality.

Security features instituted in the circuit design to protect against tampering and theft of intellectual property during the later phases of the production process

1.060 Withhold information about each component's intended use from the documentation that will be sent along with its design to those responsible for producing it.

1.061 Reserve key design components to the downloadable firmware of a chip, so that the physical chip is not functional until that firmware has been downloaded onto it.

1.062 Incorporate a design lock in the chip, so that the chip can't be employed without the key to that design lock.

© 2012 Internet Security Alliance

1.063 Create some secret performance tests with results which will not be available to the fabrication personnel or deducible by them, but which will provide a good indicator of whether the chip has been fabricated faithfully.*

1.064 Identify or create digital characteristics in the design that would be changed if the design were augmented with additional circuits.*

1.065 Recognize that having electronic components fit snuggly into their housings is an important security feature, since it hinders illicit add-ons.

Physical product design

Creation of physical circuit layouts using circuit layout software

1.066 Stringently separate the network containing the circuit layout software from other corporate networks.

1.067 Make each human operation in the application of the layout design software a two-person effort.

1.068 Check the circuit layout designs to make sure they have special features that were secretly predicted from the schematic diagrams.*

Computer-aided steps to produce physical layout of mask layers

1.069 Stringently separate the network containing the software for the physical layout of mask layers from other corporate networks.

1.070 Limit the personnel with physical and/or digital access to the network containing the software for the physical layout of mask layers.

1.071 Document the arrivals and departures of the personnel accessing the work stations connected to the network used for the physical layout of mask layers.

Transmission of wafer mask physical layouts to the wafer mask production facility

1.072 Convey the physical layouts for the wafer masks to the wafer mask production facility either (a) using a virtual private network (VPN) that allows direct instruction of the machines writing the masks, or (b) using a secure server that is being employed as a "drop box" to allow downloading of information over an encrypted connection.

1.073 If a secure server is being employed as a "drop box," make sure the information placed in it is strongly encrypted.

1.074 If a secure server is being employed as a "drop box," make sure the information in this "drop box" is erased from the server after it has been downloaded.

1.075 If a secure server is being employed as a "drop box," access to the drop box should be controlled with strong authentication measures, such as a username and token to access the drop box and then a onetime password, sent by another channel, to access the materials.

1.076 Use a different communication channel for sending the encryption key for the information being sent from the design facility to the wafer mask production facility.

1.077 Use a new encryption key for the physical layout designs of each successive product.

© 2012 Internet Security Alliance

Creation and evaluation of product prototypes

Building of prototypes

1.078 Substitute field programmable gate arrays (FPGA's) for regular components wherever possible in the building of prototypes, not just to save time and money, but also to limit the dissemination of design information.

1.079 Procure the generic components of the prototypes in an anonymous fashion, so that it would be difficult for an outsider to construct a list of what components are being used or to insert compromised components into the production of the prototype.

1.080 Make sure that there is a documented chain of custody, recording the locations, dates, times, and persons responsible for each of the critical prototype components as they are built and brought together for pre-assembly and assembly.

1.081 Do as much as possible of the molding of non-electronic components, the circuit board pre-assembly, and the actual prototype assembly within a facility fully controlled by the product designers.

Testing of prototypes

1.082 Make sure that there is a documented chain of custody, recording the locations, dates, times, and persons responsible for each completed prototype, as it is moved to different rooms or facilities in the course of the various testing procedures.

1.083 Allow only authorized personnel to have access to the prototypes, including those that are not going into production.

1.084 Document the identities, times, and circumstances of anyone accessing the prototype(s).

1.085 Include simulations of intentional attacks with the performance tests and durability tests to which the prototypes are subjected.

1.086 Make sure the test results from the prototype(s), especially the performance data, are stored and communicated in secure ways.

1.087 Take special precautions to secure the defect and vulnerability data from the prototype(s) and to limit those with access to it.

1.088 When alternative prototypes are being tested, withhold all clues as to which prototype will actually be put into production.

1.089 Destroy the obsolete prototypes in a carefully specified manner that prevents any information from being retrieved from them.

Transmission of prototype samples for production quotes

1.090 Starting the actual prototypes and prototype components, select or construct prototype samples specifically for the purpose of obtaining production quotes.

1.091 If it can be readily done, remove or modify any revealing aspects of the prototype samples that aren't necessary for producing the production quotes.

1.092 Estimate the degree of harm that would be caused by each prototype sample falling into the wrong hands prior to the start of production.

1.093 If having a given prototype sample fall into the wrong hands could cause great harm, arrange for it to be transported only by trusted couriers, operating in pairs.

© 2012 Internet Security Alliance

1.094 If a pair of trusted couriers are employed, make sure each is equipped with a personal GPS device and makes regular radio or cell phone contact.

1.095 Seal each prototype sample for shipping with tamper-revealing seals and lock it in a sturdy transport box.

1.096 Have two personnel at the destination facility verify that they have received the prototype sample with its transport box and tamper-revealing seals intact.

1.097 Limit the information that will be sent to supplement the prototype examples to that which is actually necessary for the production quotes.

1.098 Transmit the supplementary information corresponding to the prototype samples in an encrypted form and over a virtual private network (VPN).

1.099 Use a different communication channel for sending the encryption key for the supplementary information corresponding to the prototype samples.

1.100 Verify that the prototype samples are sent back using the same sort of security measures as when they were sent out.

1.101 Make sure that each prototype sample is returned complete, after the production quotes have been prepared, but before they have been accepted or rejected.

1.102 If the prototype samples are not going to be used again, make sure that they are securely destroyed.

Creation of templates and molds for the non-electronic components

1.103 Make sure the designs for the templates and molds for the non-electronic components, especially the component housings, take full account of the ways the final components might differ in size from the prototype components, so that extra spaces aren't created that would make illicit add-ons easier.

1.104 Use coded labeling for templates and molds, so that the labels do not reveal where and how the corresponding components are going to be used.

1.105 If the production of templates and molds is outsourced, arrange for them to be sent, along with test examples, to the design facility for detailed inspection before being forwarded to the production facilities.

1.106 Send the templates and molds directly from the design facility to the facilities where they are going to be used in the production of the non-electronic components.

Consolidation and clean-up of design process information

1.107 Have a small team from the corporation that owns the designs verify that the corporation has copies of all the key designs and simulation data from each stage of the design process, along with adequate explanatory notes.

1.108 As soon as it is clear that the designs will not need to be revised further and their receipt by their owner is verified, initiate a program of systematically expunging the design data from each facility used to produce the designs.

1.109 Have two information technology specialists from each design facility compile a complete list of all the places in the facility where design data might still reside, including any temporary and backup documents that might have been automatically generated by the computers used in the design process.

© 2012 Internet Security Alliance

1.110 Have an information technology specialist from each design facility, accompanied by a senior supervisor or a representative of designs' owner, perform a thorough wipe of the design data at each digital location where it might reside.

1.111 Have the information technology specialist and supervisor or representative who witnessed the data being wiped personally sign a declaration that this was done and that no further data on that product's designs reside in the facility's information systems.

1.112 Send a copy of each document testifying that the design data was wiped to the team responsible for the consolidation and clean-up of the design data.

1.113 Have all of the people who worked on the designs collect all of the paper notes, diagrams, and print-offs they used in the design process and forward them in sealed packages to the team responsible for the consolidation and clean-up of the design data.

1.114 Have the team responsible for the consolidation and clean-up of the design data verify that all the documents and data that were likely to have been created during the design process have been accounted for and dealt with properly.

2. The Photomask Production Phase

Wafer mask receiving

Receiving of mask specifications and layouts

2.001 Severely limit the personnel allowed to access the computers used to receive and handle the mask specifications and layouts.

2.002 Require two-factor authentication for any access to the computers used to receive and handle the mask specifications and layouts.

2.003 Require two authorized personnel to be present whenever sets of mask specifications and layouts are being accessed or processed.

2.004 Maintain regular logs recording which personnel access the mask specifications and layouts and at what times.

2.005 For the reception of mask data, either a) provide a connection employing an encrypted, virtual private network that allows direct instruction of the machines writing the masks, or b) download the mask specifications and layouts through an encrypted connection with a secure server that is being employed as a "drop box."

2.006 Allow no backup copies of the mask specifications and layouts at the wafer mask production facility.

2.007 If any mask data needs to be reloaded, apply to the design facility that provided it, so that a second secure transmission of the data can be arranged using the same procedures that were followed the first time.

© 2012 Internet Security Alliance

Receiving of materials and equipment for wafer mask production

2.008 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

2.009 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

2.010 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately visible.

2.011 Record each transfer of supplies from the storage cages or storage rooms to the wafer mask production areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

2.012 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the wafer mask production facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

3.013 Verify that any new equipment for the wafer mask production facility has been sent directly from the original manufacturer with tamper-revealing seal intact and with no unexplained delays or detours in its transport.

2.014 Have two trusted personnel oversee the moving and installation of equipment into the wafer mask production facility, maintaining continual, personal surveillance of the personnel carrying out this work.

2.015 Make sure any equipment from the wafer mask production facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Wafer mask production process

Wafer mask production facility physical layout and work processes

2.016 Make sure the fences, walls, and windows of the wafer mask production facility provide adequate barriers to physical intrusions.

2.017 Make sure the wafer mask production facility has only one entrance and exit in normal use.

2.018 Equip the main entry and exit with a mantrap door.

2.019 Equip emergency exits with alarms and video surveillance.

2.020 Limit the personnel with access to the wafer mask production facility to those who genuinely need to be there.

2.021 Use two or three factor authentication (e.g., photo RFID and fingerprint) for all personnel entering and leaving the mask production facility.

2.022 Document the arrivals and departures of all personnel entering the wafer mask production facility.

2.023 Plan the layout and work flow in the mask production facility so that no single person will have access to any complete set of masks.

© 2012 Internet Security Alliance

2.024 Label the masks in ways that do not reveal the sequence in which they will be applied during production.

2.025 Make sure multiple complementary masks are not subjected to repair with standard repair tools operated by the same personnel.

2.026 Arrange for random, unannounced access to the wafer mask production facility by the corporate customer or a trusted third party for inspection purposes.

Wafer mask production facility information processes

2.027 Make sure the network for the wafer mask production facility is isolated from other corporate networks.

2.028 Carry out all non-technical operations using the corporate network that is kept outside the secure rooms that are used for wafer mask production.

2.029 Make sure the wafer mask production area has no more than one access point to the internet.

2.030 Utilize non-standard, higher-number ports for the special communications coming into the wafer mask production facility.

2.031 Arrange for the firewalls though which incoming data must pass to block all types of communications and all logical ports, except those required for the main tasks of the facility.

2.032 Set the access controls in the wafer mask facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

2.033 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

2.034 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

2.035 Maintain regular logs recording which personnel access which systems and data and at what times.

2.036 Allow the network for the wafer mask production facility to be accessed only by "thin client" terminals that are not running any software applications of their own.

2.037 Physically disable all the open physical data ports on the "thin client" terminals and other equipment, so that portable memory devices cannot be plugged into them.

2.038 Track all access and distribution of the mask specifications and layouts using an automated system.

2.039 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

2.040 Make sure there is no device containing information on mask specifications and layouts that could be physically removed from the facility without great difficulty.

2.041 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the wafer mask production facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

© 2012 Internet Security Alliance

2.042 When the production of a set of wafer masks is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Wafer mask production personnel

Introduction of personnel to the wafer mask production facility

2.043 Make sure all personnel who will be admitted to the wafer mask production facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

2.044 Require a greater degree of background checks for the personnel who will be involved in the receiving and handling of mask specifications and layouts.

2.045 Require each employee in the wafer mask production facility to sign an agreement specifying that he or she has not retained documents from a previous employer containing trade secrets, confidential data, or other intellectual property.

2.046 Require each employee in the wafer mask production facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

2.047 Require each employee in the wafer mask production facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

2.048 Require each employee in the wafer mask production facility to sign an agreement specifying that he or she will not solicit or engage in business with the company's customers or suppliers for at least a year after leaving the company.

2.049 Require each employee in the wafer mask production facility to sign an agreement specifying that he or she will not recruit or hire the company's employees for at least a year after leaving the company.

2.050 Conduct entrance interviews in which each new employee in the wafer mask production facility confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

2.051 Explicitly define the limitations on the physical and digital privileges of each employee in the wafer mask production facility.

2.052 Require each employee in the wafer mask production facility to acknowledge the limitations on his or her physical and digital access privileges.

Management of personnel in the wafer mask production facility

2.053 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

2.054 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not from the same family or clan and, where practical, not from the same town or tribe.

© 2012 Internet Security Alliance

2.055 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the wafer mask production facility

2.056 Make sure that any employee discovered to be intentionally removing *any* information from the wafer mask production facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

2.057 Make sure that an employee's physical and digital access to the wafer mask production facility and its information systems is ended at the same time his or her work responsibilities inside that facility are ended.

2.058 Conduct exit interviews in which anyone who will no longer be employed by the wafer mask production facility confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that facility can be used in future jobs.

Management of finished masks

Storage and disposal of masks

2.059 Make security the major consideration in decisions about when and whether to store the masks at the mask production facility, a bonded storage facility, or some other location, when they are not being used.

2.060 Make sure that the storage vault for the masks is kept locked and that it can only be accessed by two authorized personnel.

2.061 Arrange for conspicuous labels to be promptly placed on any masks that are obsolete, due to being defective, no longer needed, or past the date up to which they need to be stored.

2.062 Use tamper-revealing materials for the labels identifying masks as obsolete.

2.063 Make sure that masks are scheduled for prompt destruction once they have become obsolete.

2.064 Break down the obsolete masks into pieces of a small, specified size when it is time to destroy them.

2.065 Require two authorized personnel to observe and verify the physical destruction of any obsolete masks, or alternatively, ship them to the owner of the intellectual property for destruction.

Shipping of finished masks

2.066 Do not ship the finished masks to the fabrication facility until the fabrication facility is almost ready to install them on the photolithography projectors.

2.067 Divide the masks from each mask set into two different packages that will be shipped separately.

2.068 Make sure that information on the sequence of layers and the specification of intervening processes (job deck view) is not shipped with the finished masks.

2.069 Seal each package for shipping with tamper-revealing seals and lock it in a sturdy transport box, separate from the remainder of the mask set.

© 2012 Internet Security Alliance

2.070 Use transport boxes equipped with GPS and radio tracking.*

2.071 Use transport boxes that will record when and where they are opened and send a radio signal transmitting this information.*

2.072 Ship the two packages containing different parts of the same mask set at different times via different vehicles.

2.073 Use two trusted couriers to transport each package of masks to the fabrication facility.

2.074 Make sure each courier is equipped with a personal GPS device and makes regular radio or cell phone contact.

2.075 Vary the schedule and route of the couriers transporting the mask shipments.

2.076 Send the information on the sequence of layers and the specification of intervening processes (job deck view) in an encrypted form and over a virtual private network (VPN).

2.077 Use a different communication channel for sending the encryption key for the information on the sequence of layers and the specification of intervening processes (job deck view).

2.078 Strictly limit the number of newly designed microchips or other electronic components that will have their sequence and process specifications sent using the same encryption key.

3. The Microelectronic Fabrication Phase

Microelectronic fabrication sourcing and receiving

Hand-off of wafer masks and fabrication specifications

3.001 Verify the identity of the delivering couriers with photographs or biometric identifiers transmitted separately, in advance.

3.002 Require two authorized people for accepting a delivery of masks.

3.003 Photograph the two delivering couriers making the hand-off to the two personnel accepting the delivery.

3.004 Document the exact time of the delivery and the non-photographic identifiers of the personnel participating in the hand-off.

3.005 Require two-factor authentication for any access to the computers used to receive and decrypt information on the sequence of layers and the intervening production processes.

3.006 Require two authorized people to be present for receiving and decrypting information on the sequence of layers and the intervening production processes (job deck view).

Sourcing and receiving of fabrication materials and generic parts

3.007 Verify that all materials and parts, including generic ones, are coming from reputable suppliers.

3.008 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

© 2012 Internet Security Alliance

3.009 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

3.010 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

3.011 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

3.012 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

3.013 Run quality checks on the material batches shortly after their delivery.

3.014 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

3.015 Record each transfer of supplies from the storage cages or storage rooms to the fabrication areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

3.016 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the fabrication facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing, receiving, and installation of microelectronic fabrication equipment

3.017 Make sure all equipment for the fabrication facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

3.018 Verify that each piece of equipment for the fabrication facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

3.019 Require a clear chain of custody for any equipment for the fabrication facility that is not being purchased directly from its manufacturer.

3.020 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

3.021 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

3.022 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

3.023 Have two trusted personnel oversee the moving and installation of equipment into the fabrication facility, maintaining continual, personal surveillance of the personnel carrying out this work.

3.024 Make sure any equipment from the fabrication facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

© 2012 Internet Security Alliance

Microelectronic fabrication processes

Physically securing the fabrication facility

3.025 Make sure the fences, walls, and windows of the fabrication facility provide adequate barriers to physical intrusions.

3.026 Make sure the fabrication area has only one entrance and exit in normal use.

3.027 Equip emergency exits with alarms and video surveillance.

3.028 Specify what types of equipment are allowed in the fabrication facility in agreement with the corporate customer.

3.029 Limit the personnel with access to the fabrication facility to those who genuinely need to be there.

3.030 Document the arrivals and departures of all personnel entering the fabrication facility.

3.031 Provide a place outside the fabrication facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

3.032 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

3.033 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the fabrication facility

3.034 Make sure the fabrication facility networks are isolated from other corporate networks.

3.035 Compartmentalize the fabrication facility networks, so that each set of equipment has access to no more of the design than necessary.

3.036 Set the access controls in the fabrication facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

3.037 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

3.038 Severely limit the information accessible to equipment maintenance personnel.

3.039 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

3.040 Maintain regular logs recording which personnel access which systems and data and at what times.

3.041 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

3.042 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

© 2012 Internet Security Alliance

Fabrication facility work processes

3.043 Restrict all personnel in the fabrication facility to the physical areas they need to enter in order to carry out their specific job assignments.

3.044 Maintain constant video surveillance of the fabrication processes with high-quality cameras that have the capability of low speed, high quality video playback.

3.045 Separate the masks, so that they are not all accessible at the same place, at the same time.

3.046 Use only automated systems for wafer transport.

3.047 Conceal from the fabrication facility personnel the identities of the customers for all components.

3.048 Arrange for random, unannounced access to fabrication facility for inspections (probably by a trusted third party, who can protect the fabrication facility's intellectual properties from its customer).

3.049 Arrange for environmental quality issues above a specified level or frequency to be automatically reported to the corporate customer.

3.050 Arrange for auditing of the fabrication facility production schedule by the corporate customer or a trusted third party to verify that there weren't any undocumented production runs.

3.051 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the fabrication facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Managing the fabrication facility supply inventory

3.052 Track the movement of supplies within the fabrication areas, using automatic scanning wherever possible.

3.053 Arrange for the material inputs of each production run to be automatically reported to the corporate customer, so that yield levels can be verified.

3.054 Make sure that all input ingredients are accounted for across successive production runs to confirm that more components weren't made than reported and that there weren't any undocumented production runs.

3.055 Make sure all defective components that are produced are delivered to the corporate customer or subjected to a documented destruction witnessed by two authorized people.

3.056 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

3.057 Carry out an immediate investigation if there are significant quantities of supplies unaccounted for at any stage and take steps to prevent this from happening again.

© 2012 Internet Security Alliance

Personnel in microelectronic fabrication

Introduction of personnel to the fabrication facility

3.058 Make sure all workers who will be admitted to the fabrication facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

3.059 Require a greater degree of background checks for the personnel who will be allowed in the testing facility or the failure analysis facility.

3.060 Require each employee in the fabrication facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

3.061 Require each employee in the fabrication facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

3.062 Require each employee in the fabrication facility to sign an agreement specifying that he or she will not solicit or engage in business with the company's customers or suppliers for at least a year after leaving the company.

3.063 Require each employee in the fabrication facility to sign an agreement specifying that he or she will not recruit or hire the company's employees for at least a year after leaving the company.

3.064 Conduct entrance interviews in which each new employee in the fabrication facility confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

Management of personnel in the fabrication facility

3.065 Explicitly define the limitations on the physical and digital privileges of each employee.

3.066 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

3.067 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

3.068 Where local conditions permit, make sure that the fabrication work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

3.069 Make sure that there are regular rotations of fabrication facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

3.070 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

3.071 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

© 2012 Internet Security Alliance

Exclusion of personnel from the fabrication facility

3.072 Make sure that any employee discovered to be intentionally removing *any* information from the fabrication facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

3.073 Make sure that an employee's physical and digital access to the fabrication facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

3.074 Conduct exit interviews in which anyone who will no longer be employed by the fabrication facility confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that facility can be used in future jobs.

Microelectronic fabrication quality control and verification tests

Routine quality testing

3.075 Adjust the frequency and severity of the quality controls, depending on the criticality of the intended product.

3.076 Keep all test equipment in a locked space or cabinet when it is not in use.

3.077 Require two authorized personnel to be present in order to unlock the space or cabinet in which the test equipment is kept.

3.078 Limit all knowledge of the specific test procedures to the few test personnel with a genuine need-to-know.

3.079 Carry out the tests using test programs that are running only on a secure test server.

3.080 Make sure the network connection with the secure test server is itself secure with encryption of all test data transmissions.

3.081 Prevent the test personnel from having any access to the test programs, apart from the test data inputs.

3.082 Limit access to the equipment for wafer probing (to make sure the probing equipment isn't used to sabotage the wafers).

3.083 Collect and secure raw data on the use of the wafer probing equipment (for audit purposes).

3.084 Erase the test data and test programs as soon as the production run for that microchip is finished, the chips have been mounted, and the finished components have been packaged for shipping.

Failure analysis and reliability testing

3.085 Physically segregate the failure analysis center from the fabrication space.

3.086 Severely limit the personnel with access to the failure analysis center.

3.087 Document the arrivals and departures of any personnel entering the failure analysis center.

3.088 Map out a strategy for failure analysis that allows the necessary tests and comparisons to be made with as few documents as possible being simultaneously accessed.

© 2012 Internet Security Alliance

3.089 Automatically track and document the person, place, and time involved in any accessing of documents for failure analysis.

3.090 Do not allow the failure analysis team members to have simultaneous access to the designs, masks, sequence of layers, specification of intervening processes, and product information.

3.091 Erase all copies of the documents used in failure analysis from the computers used in the analysis, as soon as these documents have been used for a given piece of modeling or comparison, even if this means having to retrieve them later from their source.

3.092 If the failure analysis is outsourced to a third party failure analysis lab, make sure that their security procedures are at least as stringent as the security procedures for testing and analysis done in-house.

3.093 Report the results of the failure analysis to the design team and to the customer, so that any patterns of failure that might indicate security problems can be identified.

3.094 Report the practical conclusions from the failure analysis to the relevant facility manager as well as to the manager responsible for the specific process that was deemed to be at fault.

Chip package assembly and downloading of firmware

Mounting on chip carrier

3.095 If the mounting of the chips is carried out in a separate physical facility from the fabrication of the chips, arrange for a secure transfer of the unmounted chips, with the chips under constant guard by two trusted personnel.

3.096 Visually inspect the mounted chips before they are encapsulated, in addition to any electronic tests planned or already carried out.

Encapsulation in ceramic, epoxy resin, or other plastic

3.097 Verify that resin ingredients are being added in the right proportions by putting an automated gauge and recorder on their storage reservoirs.

3.098 Make sure the encapsulation process is resulting in chips with a flawless, uniform appearance.

3.099 If possible, use an encapsulation material with distinctive optical properties.*

Downloading of firmware

3.100 If possible, download the firmware for the chip directly from a server owned and maintained by the corporate customer, so that no copies of the firmware are stored in the fabrication facility.

3.101 Make sure the electronic equipment used to download the firmware is isolated from all other networks, except, possibly, for one secure connection to a server owned and maintained by the corporate customer.

3.102 If the firmware is a source of intellectual property control or a repository of highly sensitive information, carry out the downloading of firmware at a separate unit run by the corporate customer.

3.103 Run chip functionality tests after the burn-in of the firmware.

© 2012 Internet Security Alliance

Shipping of microelectronic components

Arrangements for microelectronic component shipments

3.104 Do not store the finished microelectronic components any longer than is necessary to accumulate the quantity included in a standard shipment.

3.105 Verify that the prospective shipping company has a reputation for reliability and integrity and, if appropriate, has been accredited by the relevant authority.

3.106 Use a high-volume shipping company or a variety of shipping companies.

3.107 Ship using a receiving depot that handles many other kinds of shipments, including low value ones.

3.108 Make the packaging and labeling anonymous, so that the nature and contents of the shipments cannot be easily identified while they are in transit.

3.109 Use addresses that appear to go to different destinations for different shipments.

3.110 Use a variety of different outside package shapes and sizes.

Packaging and tracking of microelectronic component shipments

3.111 Package the electronic components in secure containers with tamper-revealing seals.

3.112 Put labels on the containers that can be automatically read (RFID's, UID's, PPID's, or, at least bar codes) and that cannot be removed without causing conspicuous damage to the shipment.

3.113 Require that the containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

4. The Circuit Board Fabrication Phase

Sourcing and receiving of circuit board materials

Sourcing and receiving of materials and generic parts

4.001 Verify that all materials and parts, including generic ones, are coming from reputable suppliers.

4.002 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

4.003 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

4.004 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

4.005 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

© 2012 Internet Security Alliance

4.006 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

4.007 Run quality checks on the material supplies shortly after their delivery.

4.008 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

4.009 Record each transfer of supplies from the storage cages or storage rooms to the circuit board fabrication areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

4.010 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the circuit board fabrication facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing and receiving of circuit board fabrication equipment

4.011 Make sure all equipment for the circuit board fabrication facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

4.012 Verify that each piece of equipment for the circuit board fabrication facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

4.013 Require a clear chain of custody for any equipment for the circuit board fabrication facility that is not being purchased directly from its manufacturer.

4.014 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

4.015 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

4.016 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

4.017 Have two trusted personnel oversee the moving and installation of equipment into the circuit board fabrication facility, maintaining continual, personal surveillance of the personnel carrying out this work.

4.018 Make sure any equipment from the circuit board fabrication facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Receiving and tooling of circuit board designs

Organization of the circuit board fabrication layout shop

4.019 Maintain a circuit board layout shop that is isolated from the rest of the circuit board fabrication facility.

4.020 Severely limit the personnel with access to the circuit board layout shop.

4.021 Document the arrivals and departures of any personnel entering the circuit board layout shop.

© 2012 Internet Security Alliance

4.022 Do not allow any employee to be inside the circuit board layout shop unless another employee is also present.

4.023 Make sure the network for the circuit board layout shop is isolated from other corporate networks and from the network for the rest of the circuit board fabrication facility.

Receiving of circuit board specifications and layouts

4.024 Arrange to have the circuit board specifications and layouts transmitted directly to the circuit board layout shop.

4.025 Arrange to receive the circuit board specifications and layouts via a virtual private network (VPN) with an additional encryption of the layout data.

4.026 Arrange to receive the encryption key via a different communication channel.

Creation of the tooling for circuit board layout

4.027 Label the tooling components in such a way that the labels do not reveal the customer or use of the boards being built.

4.028 Make sure each human operation in the application of the circuit board layout software is verified or reviewed by a second person.

4.029 Make sure the operation of the laser photoplotters is verified or reviewed by a second person.

4.030 Divide the layer images, drilling layouts, and other tooling components into different groups, so that they can be transferred to the fabrication facility separately and installed on the fabrication equipment by different personnel.

4.031 Sign each group of tooling components over to a different pair of personnel who will be responsible for installing them on the equipment in the circuit board fabrication facility.

Circuit board fabrication processes

Physically securing the circuit board fabrication facility

4.032 Make sure the fences, walls, and windows of the circuit board fabrication facility provide adequate barriers to physical intrusions.

4.033 Make sure the circuit board fabrication facility has only one entrance and exit in normal use.

4.034 Equip emergency exits with alarms and video surveillance.

4.035 Limit the personnel with access to the circuit board fabrication facility to those who genuinely need to be there.

4.036 Document the arrivals and departures of all personnel entering the circuit board fabrication facility.

4.037 Provide a place outside the circuit board fabrication facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

4.038 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

© 2012 Internet Security Alliance

4.039 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the circuit board fabrication facility

4.040 Set the access controls in the circuit board fabrication facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

4.041 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

4.042 Severely limit the information accessible to equipment maintenance personnel.

4.043 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

4.044 Maintain regular logs recording which personnel access which systems and data and at what times.

4.045 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

4.046 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management and oversight of the circuit board fabrication operations

4.047 Maintain constant video surveillance of the circuit board fabrication processes with high-quality cameras that have the capability of low speed, high quality video playback.

4.048 Keep the personnel throughout the circuit board fabrication facility from knowing how and where each batch of boards is going to be used.

4.049 Make sure personnel do not have physical access to the circuit board fabrication equipment during their breaks.

4.050 Arrange for random, unannounced access to the circuit board fabrication facility by the corporate customer or a trusted third party for inspection purposes.

4.051 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the circuit board fabrication facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

Managing the circuit board fabrication supply inventory

4.052 Track the movement of supplies within the circuit board fabrication areas, using automatic scanning wherever possible.

4.053 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

4.054 Carry out an immediate investigation if there are significant quantities of supplies unaccounted for at any stage and take steps to prevent this from happening again.

© 2012 Internet Security Alliance

Circuit board fabrication personnel

Introduction of personnel to the circuit board fabrication facility

4.055 Make sure all workers admitted to the circuit board fabrication facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

4.056 Require a greater degree of background checks for the personnel who will be allowed in the circuit board layout shop or in the circuit board testing facility.

4.057 Require each employee in the circuit board fabrication facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

4.058 Require each employee in the circuit board fabrication facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

4.059 Require each employee in the circuit board fabrication facility to sign an agreement specifying that he or she will not solicit or engage in business with the company's customers or suppliers for at least a year after leaving the company.

4.060 Require each employee in the circuit board fabrication facility to sign an agreement specifying that he or she will not recruit or hire the company's employees for at least a year after leaving the company.

4.061 Conduct entrance interviews in which each new employee in the circuit board fabrication facility confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

4.062 Explicitly define the limitations on the physical and digital privileges of each employee.

4.063 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

Management of personnel in the circuit board fabrication facility

4.064 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

4.065 Make sure that there are regular rotations of circuit board fabrication facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

4.066 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

4.067 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the circuit board fabrication facility

4.068 Make sure that any employee discovered to be intentionally removing *any* information from the circuit board fabrication facility is immediately and permanently denied all

© 2012 Internet Security Alliance

access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

4.069 Make sure that an employee's physical and digital access to the circuit board fabrication facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

4.070 Conduct exit interviews in which anyone who will no longer be employed by the circuit board fabrication facility confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that facility can be used in future jobs.

Circuit board quality control and testing

4.071 Maintain a circuit board testing facility that is isolated from the rest of the circuit board fabrication facility.

4.072 Limit the personnel with access to the circuit board testing facility and document their arrivals and departures.

4.073 Set up a special receiving system for electronic components that may need to be loaded into the boards for testing purposes.

4.074 Carry out tests of the circuit boards using generic components whenever possible, rather than the components that will be used in the actual product.

4.075 Erase the test data and test programs as soon as the production run for that circuit board is finished and all the boards have been packaged and sealed for shipping.

Circuit board shipping

4.076 Verify that the prospective shipping company has reputation for reliability and integrity.

4.077 Package the circuit boards in secure containers with tamper-revealing seals.

4.078 Notify the pre-assembly facility when they can expect the circuit boards to be delivered.

5. The Board Pre-Assembly Phase

Pre-assembly sourcing and receiving

Selection of suppliers in buying process

5.001 Compile and update profiles of potential suppliers.

5.002 Eliminate any gray market suppliers from the list of potential suppliers.

5.003 Identify and track potential spot market suppliers in case it becomes necessary to use them.

5.004 Make sure that only trusted suppliers are used for the critical components, such as processors, chip sets, memory, and downloadable firmware, especially drivers.

5.005 Make sure that suppliers whose security has been less thoroughly verified are used only for non-critical components, such as capacitors and power supplies, and for less critical materials, such as epoxies.

© 2012 Internet Security Alliance

5.006 Require the provenance of generic products to be tracked and documented, stage by stage, until their arrival.

5.007 Contractually specify the level of assurance required of each product from an outside supplier.

5.008 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

5.009 Use the data on end-user maintenance problems (supplied by the company responsible for the end product) to identify sources that may be substituting counterfeit or poorer quality components for authentic, high-quality components.

Reception and testing of incoming chips, board bases, parts, and materials

5.010 Check the documentation of the shipment tracking from the fabrication facility to the receiving center, making sure there were no unexplained delays or detours.

5.011 Store incoming supplies in locked storage cages, or locked storage rooms under constant video surveillance, that are each accessible only by two people together.

5.012 If possible, arrange for the storage cages or storage rooms to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

5.013 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that activity inside the storage areas or changes in their contents are immediately evident.

5.014 Physically inspect the received parts, looking specifically for signs of alterations and substitutions, including details of soldering, resin applications, and alignments that are less regular or less perfect than would be produced by a major production facility.

5.015 Tag the supplies and/or identify unique characteristics of the material batches that can be used to track them.

5.016 Carry out random testing of the customized microchip functions.

5.017 Verify the non-proprietary portions of the microchips, as well as the proprietary ones.

5.018 Test specifically for the sort of delayed effect degradations that could have been intentionally caused.

5.019 Record each transfer of supplies from the storage cages or storage rooms to the pre-assembly areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

5.020 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

5.021 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the pre-assembly facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

© 2012 Internet Security Alliance

Sourcing and receiving of pre-assembly equipment

5.022 Make sure all equipment for the pre-assembly facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

5.023 Verify that each piece of equipment for the pre-assembly facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

5.024 Require a clear chain of custody for any equipment for the pre-assembly facility that is not being purchased directly from its manufacturer.

5.025 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

5.026 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

5.027 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

5.028 Have two trusted personnel oversee the moving and installation of equipment into the pre-assembly facility, maintaining continual, personal surveillance of the personnel carrying out this work.

5.029 Make sure any equipment from the pre-assembly facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Processes in the pre-assembly facility

Physically securing the pre-assembly facility

5.030 Make sure the fences, walls, and windows of the pre-assembly facility provide adequate barriers to physical intrusions.

5.031 Make sure the pre-assembly facility has only one entrance and exit in normal use.

5.032 Equip emergency exits with alarms and video surveillance.

5.033 Limit the personnel with access to the pre-assembly facility to those who genuinely need to be there.

5.034 Document the arrivals and departures of all personnel entering the pre-assembly facility.

5.035 Provide a place outside the pre-assembly facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

5.036 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

5.037 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

© 2012 Internet Security Alliance

Control of information systems in the pre-assembly facility

5.038 Set the access controls in the pre-assembly facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

5.039 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

5.040 Severely limit the information accessible to equipment maintenance personnel.

5.041 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

5.042 Maintain regular logs recording which personnel access which systems and data and at what times.

5.043 Make sure the pre-assembly production area has no more than one access point to the internet.

5.044 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

5.045 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management of pre-assembly facility operations

5.046 Restrict all personnel in the pre-assembly facility to the physical areas they need to enter in order to carry out their specific job assignments.

5.047 Stamp each circuit board with a unique serial number before beginning to add components to it.

5.048 Set a work time schedule for the moving conveyer belt of circuit boards that leaves personnel with no time for mischief.

5.049 Keep the people on the line from knowing how and where the circuit board being loaded is going to be used.

5.050 Make sure personnel do not have physical access to the pre-assembly equipment during their breaks.

Oversight of pre-assembly activities

5.051 Maintain constant video surveillance of the assembly line with high-quality cameras that have the capability of low speed, high quality video playback.

5.052 Set up a system for correlating the video surveillance images with the specific circuit boards being assembled.*

5.053 Arrange for random, unannounced access to the pre-assembly facility by the corporate customer for inspection purposes.

5.054 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the pre-assembly facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

© 2012 Internet Security Alliance

Managing the pre-assembly facility supply inventory

5.055 Make sure the transfer of supplies from the storage cages or storage rooms in the pre-assembly facility reception area is carried out at a rate that makes it easy to oversee the handling of the supplies.

5.056 Track the movement of supplies and unfinished boards within the pre-assembly production areas, using automatic scanning wherever possible.

5.057 Arrange for the tracking system to generate automatic warnings if there are significant discrepancies between the quantities of supplies and unfinished boards reported at one stage of the pre-assembly process and the quantities reported at other stages.*

5.058 Immediately investigate any unexplained discrepancies in the quantities of supplies and unfinished boards, paying as much attention to extra items as to shortages.

5.059 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

5.060 If significant quantities of supplies are still unaccounted for after an investigation, institute improved surveillance and/or improved tracking to prevent this from happening again.

Testing and repair of loaded circuit boards

5.061 Keep all test equipment in a locked cage or cabinet when it is not in use.

5.062 Require two authorized personnel to be present in order to unlock the cage or cabinet in which the test equipment is kept.

5.063 Download the testing information directly from the corporate customer to the specific on-site computers that are used to carry out the tests of the loaded circuit boards.

5.064 Provide extra testing for loaded boards that are intended as replacements and that won't be going through testing at the assembly stage.

5.065 Physically tag any loaded boards that the tests indicate need repair, so that they are easy to distinguish, if possible indicating with the tags what sort of repairs are required.

5.066 Scan the serial numbers of the boards tagged as needing repair, so that they are provided with special tracking that includes extra monitoring.

5.067 Place loaded boards that need repair into a special storage space adjoining the testing area that can be locked whenever there aren't test personnel in attendance.

5.068 Scan the boards awaiting repair when they are removed from the storage space adjoining the testing area.

5.069 Transfer the boards that need repair in manageable-sized batches to a separate repair area or a separate repair facility where all incoming and outgoing parts and materials can be monitored.

5.070 Track the movement of all replacement parts into the repair area.

5.071 Track the movement of all defective or discarded parts out of the repair area and collect the higher value parts for return or special monitored disposal.

5.072 Verify that the repaired boards are returned for another round of testing when all the repairs have been completed.

5.073 Erase the test data and test programs as soon as the circuit boards in that production run have all been fully loaded with their components and made ready for shipping.

© 2012 Internet Security Alliance

Personnel in pre-assembly

Introduction of personnel to the pre-assembly facility

5.074 Make sure all workers admitted to the pre-assembly facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

5.075 Require a greater degree of background checks for the personnel who will handle testing and quality control.

5.076 Require each employee in the pre-assembly facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

5.077 Require each employee in the pre-assembly facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

5.078 Explicitly define the limitations on the physical and digital privileges of each employee.

5.079 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

Management of personnel in the pre-assembly facility

5.080 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

5.081 Make sure that workers in the pre-assembly facility are not exposed to dangerous levels of toxic substances.

5.082 Make sure that workers in the pre-assembly facility are not under fourteen years old.

5.083 Make sure that there are regular rotations of pre-assembly facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

5.084 Make sure that the workers on the assembly line are periodically reassigned to different positions, so that they do not have the same persons next to them.

5.085 Where local conditions permit, make sure that the pre-assembly work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

5.086 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

5.087 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the pre-assembly facility

5.088 Make sure that any employee discovered to be intentionally removing *any* information from the pre-assembly facility is immediately and permanently denied all access to the

© 2012 Internet Security Alliance

facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

5.089 Make sure that an employee's physical and digital access to the pre-assembly facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

Shipping of circuit boards to assembly facility

Packaging and dispatching of loaded circuit board shipments

5.090 Verify that the prospective shipping company has reputation for reliability and integrity.

5.091 Package the loaded circuit boards in secure containers with tamper-revealing seals.

5.092 Put labels on the containers that can be automatically read (RFID's, PPID's, or, at least bar codes) and that cannot be removed without causing conspicuous damage to the shipment.

5.093 Require that the containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

6. The Product Assembly Phase

Assembly sourcing and receiving

Selection of suppliers in buying process

6.001 Compile and update profiles of potential suppliers.

6.002 Eliminate any gray market suppliers from the list of potential suppliers.

6.003 Identify and track potential spot market suppliers in case it becomes necessary to use them.

6.004 Require the provenance of generic products to be tracked and documented, stage by stage, until their arrival.

6.005 Make sure that only trusted suppliers are used for the critical components, such as circuit boards, hard drives, the BIOS, and downloadable firmware, especially drivers.

6.006 Verify the choice of any suppliers of critical components with the corporate customer, especially if there is a prospective change in one of these suppliers.

6.007 Make sure that suppliers whose security has been less thoroughly verified are used only for non-critical components, such as capacitors and power supplies, and for less critical materials, such as epoxies.

6.008 Contractually specify the level of assurance required of each product from an outside supplier.

6.009 Require any outside suppliers who cannot be rapidly replaced by other suppliers to report periodically the quantity of future shipments they will be able to make from inventory if their production is interrupted.

© 2012 Internet Security Alliance

6.010 Use the data on end-user maintenance problems (supplied by the company responsible for the end product) to identify sources that may be substituting counterfeit or poorer quality components.

Reception and testing of incoming boards, parts, and materials shipments

6.011 Check the documentation of the shipment tracking from each pre-assembly facility to the receiving center.

6.012 Verify that the tracking records of the circuit board shipments from a pre-assembly facility do not have any unexplained delays or detours.

6.013 Verify the integrity of the tamper-revealing seals on the shipping containers.

6.014 Store incoming supplies in locked storage cages or storage rooms that are each accessible only by two people together.

6.015 If possible, arrange for the storage cages to be only opened by the simultaneous application of two keys or biometric identifiers to two electronic locks that are physically beyond the reach of a single person.

6.016 Make sure that the view into the storage cages is unobstructed or that the video feed from the storage rooms is constantly monitored, so that changes in their contents or activity inside them is immediately visible.

6.017 Physically inspect the incoming boards and other components, looking specifically for signs of alterations and substitutions, including details of soldering, resin applications, and alignments that are less regular or less perfect than would be produced by a major production facility.

6.018 Verify that all critical components have identifying serial numbers and make sure that these are correctly recorded.

6.019 Carry out random testing of the incoming circuit boards and other critical components.

6.020 Test specifically for the sort of delayed effect degradations that could have been intentionally caused.

6.021 Record each transfer of supplies from the storage cages or storage rooms to the assembly areas, noting the identity or type of supplies, the quantity, the time, and the two people making the transfer.

6.022 Arrange for automatic customer notifications if the inventories of designated hard-to-replace critical supplies drop below specified levels.

6.023 Compare the types and quantities of supplies leaving the storage cages or storage rooms to the outputs of the assembly facility to make sure that the quantities of outputs account for the quantities of supplies consumed.

Sourcing and receiving of assembly equipment

6.024 Make sure all equipment for the assembly facility is purchased only from trusted suppliers with a transparent corporate identity and a known business history.

6.025 Verify that each piece of equipment for the assembly facility was sent directly from the supplier with no unexplained delays or detours in the shipping route.

6.026 Require a clear chain of custody for any equipment for the assembly facility that is not being purchased directly from its manufacturer.

© 2012 Internet Security Alliance

6.027 Verify with the original manufacturer the authenticity of any important pieces of equipment purchased from a third party, even if that third party is considered a trusted supplier.

6.028 Make sure any newly arrived equipment is kept in a locked storage space prior to installation.

6.029 Have each newly arrived piece of equipment inspected inside and out by a trusted expert familiar with such equipment and make sure that the expert can account for the presence and features of each observable component.

6.030 Have two trusted personnel oversee the moving and installation of equipment into the assembly facility, maintaining continual, personal surveillance of the personnel carrying out this work.

6.031 Make sure any equipment from the assembly facility that is being replaced and that can store information has any information it might contain securely wiped or removed.

Product assembly processes

Physically securing the assembly facility

6.032 Make sure the fences, walls, and windows of the product assembly facility provide adequate barriers to physical intrusions.

6.033 Make sure the product assembly area has only one entrance and exit in normal use.

6.034 Equip emergency exits with alarms and video surveillance.

6.035 Limit the personnel with access to the assembly facility to those who genuinely need to be there.

6.036 Document the arrivals and departures of all personnel entering the assembly facility.

6.037 Provide a place outside the product assembly facility, where workers can check their cell phones, music players, pocket knives, and other devices that are not allowed into the facility.

6.038 Scan both *incoming* and outgoing workers for memory devices, wireless transmitters or receivers, digital cameras, counterfeit parts, mechanical tools, and other items that could have improper purposes.

6.039 Arrange for any outside personnel carrying out equipment maintenance or upgrades to be escorted and supervised at all times by a trusted employee familiar with the sort of procedures that are being carried out.

Control of information systems in the assembly facility

6.040 Set the access controls in the assembly facility's information systems so that they only allow an employee to access the systems and data deemed necessary for that employee's work assignment.

6.041 Limit supervisors' digital privileges, especially their ability to access and alter any automated logs or activity records.

6.042 Severely limit the information accessible to equipment maintenance personnel.

6.043 Change the access controls for an employee as soon as a change in work assignment makes different privileges appropriate.

© 2012 Internet Security Alliance

6.044 Maintain regular logs recording which personnel access which systems and data and at what times.

6.045 Arrange for any abnormally large downloads of information to be automatically interrupted and flagged for urgent security attention, unless there is specific authorization by a supervisor.

6.046 When the production run is finished, perform a secure wipe of all devices containing the data that was used, with two authorized personnel observing the procedure and verifying that it was done correctly.

Management of assembly facility operations

6.047 Restrict all personnel in the assembly facility to the physical areas they need to enter in order to carry out their specific job assignments.

6.048 Exclude any equipment from the product assembly facility that could be used to capture and steal intellectual property, including large and fixed-location equipment.

6.049 Make sure that the contract identification numbers cannot be easily used to identify specific customers.

6.050 Make sure each chassis has a unique product serial number indelibly inscribed on it before beginning to add components to it.

6.051 Make sure that the contract numbers and the identification numbers on the individual product items cannot be used to identify specific customers.

6.052 Prevent the people on the assembly line from learning where the computer or other finished equipment is going from *sources other than* the (anonymous) contract and product numbers.

6.053 Set a work time schedule for the moving conveyer belt of product items being assembled that leaves personnel with no time for mischief.

6.054 Make sure personnel do not have physical access to the assembly equipment during their breaks.

Oversight of assembly activities

6.055 Maintain constant video surveillance of the assembly line with high-quality cameras that have the capability of low speed, high quality video playback.

6.056 Set up a system for correlating the video surveillance images with the specific product items being assembled.

6.057 Scan the video for situations where the assembly line personnel seem to be doing something that doesn't correspond to their normal work movements and investigate those situations, if necessary inspecting the product items involved.

6.058 Carry out random inspections of product items for signs that components were altered or extra components inserted.

6.059 Arrange for random, unannounced access to the assembly facility by the customer for inspection purposes.

6.060 Carry out an immediate investigation if there is reason to believe someone has improperly accessed or stolen any competitively sensitive information used in the product assembly facility and, depending what is uncovered, bring appropriate remedial, employment, and/or legal action.

© 2012 Internet Security Alliance

Managing the assembly facility supply inventory

6.061 Make sure the transfer of supplies from the storage cages or storage rooms in the assembly facility reception area is carried out at a rate that makes it easy to oversee the handling of the supplies.

6.062 Track the movement of supplies within the assembly areas, using automatic scanning wherever possible.

6.063 Arrange for the tracking system to generate automatic warnings if there are significant discrepancies between the quantities of supplies and unfinished boards reported at one stage of the pre-assembly process and the quantities reported at other stages.*

6.064 Immediately investigate any unexplained discrepancies in the quantities of supplies and partially assembled products, paying as much attention to extra items as to shortages.

6.065 Arrange for regular audits at unpredictable times of the supply inventories and of the tracking data on parts and materials.

6.066 If significant quantities of supplies are still unaccounted for after an investigation, institute improved surveillance and/or improved tracking to prevent this from happening again.

Loading of final firmware and software

6.067 If possible, download the final firmware, the BIOS, drivers, and other pre-installed software directly from a server owned and maintained by the corporate customer, so that no copies are stored in the assembly facility.

6.068 Make sure the electronic equipment used to download the final firmware, the BIOS, drivers, and other pre-installed software is isolated from all other networks, except, possibly, for one secure connection to a server owned and maintained by the corporate customer.

6.069 Specify fully the functions that are to be turned off in order to customize the BIOS.

6.070 Verify by random tests that the appropriate functions were turned off in the BIOS.

6.071 If the customer determines these software programs are sufficiently critical, send product items to a physically separate facility run or supervised by the customer for the reflashing of the bios and the downloading of specialty programs.

6.072 Run chip functionality tests (J-tag ports) after the burn-in of the additional firmware.

Personnel in product assembly

Introduction of personnel to the assembly facility

6.073 Make sure all personnel admitted to the assembly facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

6.074 Require a greater degree of background checks for the assembly facility personnel who will be involved in quality control testing, repairs, the downloading of software or firmware, or post-pack testing.

6.075 Require each employee in the product assembly facility to sign a non-disclosure agreement specifying that no trade secrets, confidential data, or other intellectual property acquired or created on this job will be disclosed to people unauthorized to access them, including fellow employees.

© 2012 Internet Security Alliance

6.076 Require each employee in the product assembly facility to sign an agreement specifying that no knowledge of trade secrets, confidential data, or other intellectual property acquired or created on this job will be used in subsequent work for other employers.

6.077 Require each employee in the product assembly facility to sign an agreement specifying that he or she will not engage in business with the company's customers or suppliers for at least a year after leaving the company.

6.078 Require each employee in the product assembly facility to sign an agreement specifying that he or she will not solicit or hire the company's employees for at least a year after leaving the company.

6.079 Conduct entrance interviews in which each new employee in the assembly facility confirms his or her understanding that no trade secrets, confidential data, or other intellectual property from previous employers can be used on this new job.

6.080 Explicitly define the limitations on the physical and digital privileges of each employee.

6.081 Require each employee to acknowledge the limitations on his or her physical and digital access privileges.

Management of personnel in the assembly facility

6.082 Formally acknowledge the changes in access privileges that occur when personnel change work assignments.

6.083 Make sure that workers in the assembly facility are not exposed to dangerous levels of toxic substances.

6.084 Make sure that workers in the assembly facility are not under fourteen years old.

6.085 Make sure that there are regular rotations of assembly facility supervisory personnel, so that the same supervisor does not spend many weeks in the same physical position with the same responsibilities.

6.086 Make sure that the workers on the assembly line are periodically reassigned to different positions, so that they do not have the same persons next to them.

6.087 Where local conditions permit, make sure that the assembly work force contains at least a few people, scattered across various positions, who are not from the same clan, town, or tribe, and who have worked for the firm less than three years, so that improper collusion between workers is made more difficult.

6.088 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not consistently from the same family or clan and, where practical, not from the same town or tribe.

6.089 Make sure that whenever two people are required to perform a procedure jointly for security reasons, they are not kept together as a pair, but are rotated among other partners.

Exclusion of personnel from the assembly facility

6.090 Make sure that any employee discovered to be intentionally removing *any* information from the product assembly facility is immediately and permanently denied all access to the facility, unless further access is being intentionally allowed under surveillance as part of a criminal investigation.

© 2012 Internet Security Alliance

6.091 Make sure that an employee's physical and digital access to the product assembly facility and its information systems is ended at the same time his or her work responsibilities inside the facility are ended.

6.092 Conduct exit interviews in which anyone who will no longer be employed by the product assembly facility confirms his or her understanding that *no* knowledge of trade secrets, confidential data, or other intellectual property acquired or created during work for that facility can be used in future jobs.

Product assembly testing and repairs

6.093 Keep all test equipment in a locked cage or cabinet when it is not in use.

6.094 Require two authorized personnel to be present in order to unlock the cage or cabinet in which the test equipment is kept.

6.095 Make sure that testing is automated as much as possible, so that it is more difficult to insert extra components at the testing stage.

6.096 Monitor the activities of the test personnel with extra video surveillance.

6.097 Make sure the testing equipment is locked in read-only mode, so that new instructions cannot be easily added.

6.098 Carry out twenty-four hour functional testing of all servers being assembled at the facility.

6.099 Carry out extensive, but less lengthy testing of all personal computers and other electronic products being assembled.

6.100 Periodically carry out hash-like tests and other design fingerprint tests supplied by the product design team to verify that the product has remained faithful to its design.*

6.101 Physically tag any assembled products that the tests indicate need repair, so that they are easy to distinguish, if possible indicating with the tags what sort of repairs are required.

6.102 Scan the serial numbers of the assembled products tagged as needing repair, so that they are provided with special tracking that includes extra monitoring.

6.103 Place products that need repair into a special storage cage or storage room adjoining the testing area that can be locked whenever there aren't test personnel in attendance.

6.104 Scan the products needing repair when they are removed from the special storage cage or storage room that adjoins the testing area.

6.105 Maintain a separate repair area or separate facility for repairing assembled products where all incoming and outgoing parts and materials can be readily monitored.

6.106 Make sure the products needing repair are never left unattended when they are being transfered from the storage cage or room adjoining the testing area to the repair area.

6.107 Scan the products that need repair again when thay are delivered to the separate repair area.

6.108 Track the movement of all replacement parts or replacement assemblies into the repair area or repair facility.

6.109 Track the movement of all defective or discarded parts out of the repair area and collect the higher value parts for return or special monitored disposal.

6.110 Return any defective pre-assembled components to the facilities that manufactured them.

© 2012 Internet Security Alliance

6.111 Make sure the repaired products are returned for another round of testing when the repairs have been completed.

6.112 Erase the test data and test programs for the product as soon as the production run for that product is finished and all the products that were produced have been made ready for shipping.

Product assembly outputs

Packaging and sealing of products

6.113 Have the keys that reveal which individual product numbers will receive which labels and packaging sent directly to the merge center in an encrypted form.

6.114 Make sure each layer of product packaging is designed and applied in such a way that the packages cannot be readily opened and then resealed without leaving signs that this was done.

Random testing of products after packaging

6.115 Make sure the selection and removal of packaged products for post-pack testing is genuinely random and that the choice of items does not follow any list or schedule made out in advance.

6.116 Carry out the post-pack testing in a cage or room that is physically separate, so that all products, packaging materials, and other items going in and out can be monitored.

6.117 Take extra precautions to make sure that electronic components which could contain malicious firmware are not smuggled into the post-pack testing area.

6.118 Maintain constant video surveillance of the post-pack testing area with high quality cameras.

6.119 Require two personnel to be present for all unpacking, disassembly, inspection, testing, reassembly, and repacking of each assembly product.

6.120 Make a thorough search for unauthorized additions or substitutions of components an important part of the post-pack inspection and testing.

6.121 Verify that the unique serial numbers and other tags on the components are the exact ones that should be present in that assembly product.

6.122 Make sure that the post-pack testing personnel do not let the complete product out of their custody and sight until it is resealed.

Shipping of products

6.123 Make sure that any labels indicating whom the product is for are among the last things added at the merge center.

6.124 Seal the products in bulk shipping containers that have tamper-revealing seals and RFID's.

6.125 Require that the bulk containers be scanned and their locations reported, each time they are unloaded from a transport vehicle or loaded into one.

© 2012 Internet Security Alliance

7. The Product Distribution Phase

Secure receiving and storage of bulk product shipments

7.001 Check the documentation of each delivery, including the ID of the person making the delivery, and record the delivery data.

7.002 Verify that the tracking records of the container shipments from the assembly facility to the distribution facility do not have any unexplained delays or detours.

7.003 Make sure the space in which the bulk shipment is initially stored is secure.

7.004 Use the data on end-user maintenance problems to identify shipping avenues that may be concealing substandard physical environments or substituting counterfeit products.

Breakdown into individual product orders

Bulk container breakdown and relabeling of product units

7.005 Scan the products at each major stage of processing in the distribution facility, so that their location is always known and recorded.

7.006 Carry out a constant, automated comparison of the bulk shipments entering the facility, the products in the facility, and the products leaving the facility, so that any discrepancies are immediately detected.

Reshipment to middlemen or end users

7.007 Label each shipment with tracking information that cannot be removed without causing conspicuous damage to the shipment.

7.008 Record the handover of products to the reshipper or transporter, documenting the identities of the personnel on both sides.

Management of product sales force

7.009 Design the advance product descriptions provided to the sales force, so that certain key details about the new product are withheld until the product shipping date.

7.010 If advance samples or mock-up products are going to be provided to the sales force, make sure these have unique serial numbers.

7.011 Require the sales force members to sign for the advance samples or mock-up products and track exactly which sales force members have custody of them at all times.

7.012 Collect the advance samples or mock-up products when the real products become available and verify that all are accounted for.

Management of relationships with middlemen

7.013 Make cooperation with the manufacturer's security measures and security investigations one of the conditions for being an authorized dealer.

7.014 Require authorized dealers to buy the manufacturer's products either directly from the manufacturer or from authorized wholesalers.

7.015 Provide a secure website for customers that makes it easy to find authorized dealers and to check whether a given dealer is an authorized one.

© 2012 Internet Security Alliance

7.016 Carry out joint promotional campaigns with authorized dealers, in order to encourage customers to make their purchases from these authorized dealers.

7.017 Make it easy for dealers to report possible signs of counterfeit products or product tampering and provide them with a sufficient incentive for doing so.

7.018 Require authorized dealers to report the unique serial numbers of any large purchases that were delivered to customers and later returned.

7.019 Provide a system for tracking the provenance of any products that an authorized dealer needs to sell back to wholesalers, especially when the authorized dealer is going out of business.

End-user customer delivery and registration

7.020 Inform end-user customers persuasively of the benefits they will receive from registering the product, allowing updates and upgrades, and providing notification of the product being taken out of service.

7.021 Have end-user customers report a unique product serial number to the product registration website.

7.022 Verify the date of delivery to the end-user customer and the identity of that customer.

7.023 Notify customers immediately if their purchase appears to have been from an unauthorized dealer or if the product they purchased had been previously sold and returned.

8. The Product Maintenance and Disposal Phase

Training of product maintenance personnel

Routine handling of maintenance information

8.001 Withhold intellectual property from maintenance agents who don't need to know it.

8.002 Withhold detailed information about hardware vulnerabilities until remedial measures are being deployed.

8.003 Establish a system for bringing security issues to the attention of security personnel and for making the measures needed to deal with them a high priority.

8.004 If remedial measures cannot be made immediately available to eliminate a security issue, warn maintenance personnel about the symptoms of that security issue.

Advance training for unreleased new products

8.005 Institute strict controls on which personnel have access to the advance training materials.

8.006 Design the advance training, so that certain key details about the new product can be withheld until the product shipping date.

© 2012 Internet Security Alliance

Special training in security issues

8.007 Make security training a requirement for all maintenance personnel, just as mastery of other maintenance procedures is a requirement.

8.008 Require the maintenance personnel to respond *actively* to security training, verifying that they have grasped the key principles involved.

Updates to product

8.009 Offer regular updates or upgrades of final software for free, so that product users have an incentive to check in periodically.

8.010 Make sure that product users can access the upgrades in a secure manner with appropriate verification of electronic certificates.

8.011 Provide the product users with safe and efficient means of testing the upgrades for compatibility, usually by facilitating downloads to test environments.

Servicing of product

Protecting the product user's information and security during maintenance procedures

8.012 Limit the privileges required for remote monitoring and trouble-shooting to those genuinely necessary.

8.013 Provide product users with an easy and secure way of vetting of maintenance personnel.

8.014 Establish maintenance procedures that encourage product users to control strictly the access privileges of the maintenance personnel and to verify that the maintenance personnel are doing what they should.

8.015 Stringently protect any private product user data that must be collected to perform maintenance tasks.

8.016 Do not have the maintenance personnel retain any product user data they collect or access during maintenance procedures unless the customer agrees that the gains to both parties from retaining this information will be greater than the risks.

8.017 Encourage the removal the memory media from any product that is being sent back for repair (and make sure the warranties are written to allow this).

Carrying out secure maintenance and repairs

8.018 Scan both incoming and outgoing maintenance workers to make sure that no potentially insecure or counterfeit components are being brought in and that no authentic components are being improperly removed.

8.019 Record the descriptive label, serial number, and supply source for all replacement parts being brought into the facility where repairs are being performed.

8.020 Verify that any replacement components have gone through the same rigorous supply chain controls and testing as those built into the original product.

8.021 Record the descriptive label and serial number of all parts taken out of the facility where repairs were being performed, including the parts that were damaged and had to be replaced.

8.022 Arrange for the secure destruction or documented recycling of all damaged parts.

© 2012 Internet Security Alliance

8.023 Record the unique serial number of the product being repaired, the type of each major repair, and any replacement parts that were used, and send this information to the company that produced the product.

Protecting end-user customer identities where this is needed for security reasons

8.024 Establish a system of extra-secure maintenance providers who have had special background checks and extra training in the relevant security procedures.

8.025 Have blind-buy end-user customers establish a false-identity enterprise for the administration and billing of support services.

8.026 Have blind-buy end-users with special security needs switch to a secure maintenance provider after purchase, rather than contacting the normal maintenance centers.

Returns for resale or refurbishment

Reception of return shipments from customers and other components

8.027 Authorize each return shipment before it is sent back, noting the reported serial numbers, sales dates, reported condition, reason for return, and amount of credit requested.

8.028 Designate an authorized carrier to transport the return shipment in a reliable and secure manner.

8.029 Make sure the pick up and delivery of the return shipment are recorded, with the exact times and the identities and signatures of the personnel involved in the handovers at each end.

8.030 Maintain a secure area for the unloading and loading of shipments, with video surveillance, high fences, and a secure gate separating the area from outside parking lots and roads.

8.031 Inspect each incoming shipment within twenty-four hours of its arrival to verify that the contents and serial numbers, the physical condition of the equipment, and the condition of any factory equipment seals are exactly as reported.

8.032 Examine the high-value components in each incoming product to verify that they are all present and authentic.

8.033 Inspect the incoming products to verify that no extra electronic components have been added.

8.034 Carefully inspect any additional used parts that are being purchased to make sure that they give every sign of being from authentic branded products and are not counterfeits or inferior substitutions.

8.035 Check the original part numbers and serial numbers of any additional used parts that are being purchased and compare these to the manufacturing records to make sure that there are no inconsistencies that would suggest that the parts are counterfeits.

8.036 If the additional used parts being purchased are from authentic brand-name products, but from another manufacturer, make sure that these parts are from products with an a quality level as high as or higher than the product they will be used to refurbish.

8.037 Make sure that the used parts are of a similar or lower age and have a similar or lower degree of wear than the used products into which they will be installed.

© 2012 Internet Security Alliance

8.038 Store any products or components that are of high value and easy to move in a locked storage cage or a locked room under constant video surveillance.

8.039 Give only a very small number of senior supervisors the ability to unlock the cage or room used to store the products and components that are of high value and easy to move.

8.040 If the returned product is being shipped directly to another customer, re-package it and reseal it in a way that will make it apparent if the product package is opened again before reaching the next customer.

8. 041 Provide an extra label on each returned product that will be shipped to another customer, noting that it was opened by a previous customer, re-inspected, and re-sealed.

Management of the refurbishment or re-manufacturing processes

8.042 Make sure the fences, walls, and windows of the re-manufacturing facility provide adequate barriers to physical intrusions.

8.043 Make sure the re-manufacturing facility has only one entrance and exit in normal use.

8.044 Limit the personnel with access to the re-manufacturing facility to those who genuinely need to be there.

8.045 Make sure all personnel admitted to the re-manufacturing facility are given a basic background check, making use of financial identifiers, employment histories, and any criminal or court records that are available.

8.046 Document the arrivals and departures of all personnel entering the re-manufacturing facility.

8.047 Scan both *incoming* and outgoing personnel for electronic parts and devices.

8.048 Maintain constant video surveillance of the work spaces inside the re-manufacturing facility with high-quality cameras that have the capability of low speed, high quality video playback.

8.049 Severely limit the number of personnel in the re-manufacturing facility who have access to the computer networks used to keep track of the incoming products, the work orders, the inventories on hand, and the outgoing products.

8.050 Track the movement of returned products and critically important replacement components within the re-manufacturing facility, so that their sources, exact nature and features, current locations, and destinations can all be identified at any time.

8.051 Keep the identities of the customers for the re-manufactured products secret from the re-manufacturing facility personnel and store this information separately from the work orders.

8.052 Verify that the quantity of discarded components sent away for recycling exactly matches the quantity of replacement components brought in for the re-manufacturing processes.

8.053 Make sure the testing that the re-manufactured product undergoes before being packed for shipment is not carried out by the same personnel who worked on the product during its refurbishment.

8.054 Use the tracking information on each returned product and on each critically important replacement component to identify the sources of any problems identified in the final testing of the refurbished products.

© 2012 Internet Security Alliance

8.055 Check to make sure that all memory components in the re-manufactured product have been thoroughly wiped of any information that may have been stored in them during previous use.

8.056 Add the shipping labels that identify the customers for the re-manufactured products only after those products are packed, sealed, and ready for shipment.

8.057 Have the encrypted information that reveals which orders go to which customers sent directly to a shipping area computer *after* a designated employee has confirmed that the shipment is ready for shipping.

8.058 Make sure that an employee's access to the re-manufacturing facility is ended at the same time his or her work responsibilities inside the facility are ended.

Disposal of end-of-life-cycle products

Tracking of product disposal by the product manufacturer

8.059 Provide the product user with an incentive to inform the manufacturer when the product is taken out of service.

8.060 Provide the product user with an incentive to return the end-of-life electronic product to a manufacturer's agent for recycling.

8.061 Make it easy for the product user to provide the manufacturer with the relevant information about the product's disposal if it is not returned to a manufacturer's agent for recycling.

8.062 Maintain a centralized product registry, incorporating information about products taken out of service, including the product serial numbers, the date each product was taken out of service, the place and manner of disposal, and the date of disposal.

Management of product disposal by the product end-user

8.063 Inform the manufacturer's product registry when the product is taken out of service, so that its registration is voided.

8.064 Identify to the manufacturer the intended type of disposal, specifically whether the product is intended for resale, for remanufacturing, or for physical destruction.

8.065 Promptly remove the memory components from any product that is being taken out of service.

8.066 Perform a secure wipe of any memory components from the product being taken out of service and reflash any customized burned-in memory.

8.067 If appropriate, degauss or physically destroy, not just the memory components, but all components that could retain information from their specific use.

8.068 Whenever practical, return the product to a manufacturer's agent for recycling.

8.069 If the product is not being returned to a manufacturer's agent for recycling, remove the manufacturer's trademark and serial numbers from the product.

© 2012 Internet Security Alliance

Recycling of end-of-life products by a manufacturer's agent

8.070 Record exactly what products were returned for re-cycling, both by end-user customers and by other manufacturer facilities, noting the specific serial numbers where available.

8.071 Choose different disposal plans, depending on whether the items being recycled are products in development, outdated products, worn-out products, counterfeit products, or defective products.

8.072 Make sure that all counterfeit products and all products in development that have been sent to the recycling facility are physically destroyed.

8.073 Remove the memory components from the product if the last end-user has not done so.

8.074 Perform a secure wipe of any memory components that are not being physically destroyed and reflash any burned-in memory.

8.075 Carry out random testing of any memory components that are not being physically destroyed to verify that any information they might have contained has been successfully wiped.

8.076 Remove and securely destroy all manufacturer brand labels, serial number plates and stampings, and product casings with distinctive stylings.

8.077 Make sure that the breakdown of any components that will be re-used is complete enough, so that they cannot be resold as branded components.

8.078 Make sure that workers in the recycling facilities are not exposed to dangerous levels of toxic substances.

8.079 Make sure that workers in the recycling facilities are not under fourteen years old.

8.080 Make sure that any components that will be physically destroyed have their constituent materials recycled or disposed of in an environmentally safe manner.

9. The Necessary Legal Conditions

National laws and legal framework

Basic laws and legal principles that need to be operating

9.001 Foreigners and foreign corporations should be able to pursue legal actions, both civil and criminal, on a comparable footing with local citizens and local corporations.

9.002 Information obtained from an analysis of computer logs and other electronic records, as long as they are maintained in the regular course of business and there is a proper chain of custody, should be recognized as competent evidence in court cases.

9.003 The theft of trade secrets, confidential data, or other intellectual property should be recognized as fully comparable to the theft of other valued goods.

9.004 The intellectual properties that an employee produces during work for a corporation should be recognized as belonging to that corporation and not to the employee.

9.005 Employee non-disclosure agreements should be recognized as valid, binding, and enforceable.

© 2012 Internet Security Alliance

9.006 Post-employment restrictions on the use and disclosure of confidential and proprietary information should be recognized as valid, binding, and enforceable.

9.007 Post-employment restrictions on soliciting or engaging in business with a company's customers or suppliers should be recognized as valid, binding, and enforceable.

9.008 Post-employment restrictions on recruiting or hiring the company's employees should be recognized as valid, binding, and enforceable.

9.009 Unauthorized intrusion into the information systems of another organization or person, whether it is accomplished locally or remotely, should be recognized as a criminal offense.

9.010 Unauthorized interception or alteration of confidential communications between information systems should be recognized as a criminal offense.

9.011 The production, sale, or distribution of tools for carrying out unauthorized intrusions into information systems or for intercepting or altering confidential communications between them should be recognized as a criminal offense.

9.012 The willful infringement of copyright, including the copyright of software and data bases, should be recognized as a criminal offense.

9.013 The counterfeiting of electronic components or devices should be recognized as a criminal offense.

9.014 The intentional misrepresentation of electronic devices or software offered for sale, including the substitution of inferior or counterfeit goods, should be recognized as a criminal offense.

9.015 In addition to the direct damage suffered by the purchaser of misrepresented goods, the legal system should recognize the indirect damages suffered by the corporation whose intellectual properties and reputation were being exploited.

Aspects of local laws that could affect security procedures

9.016 There should be sufficient access to financial records, past employment histories, criminal records, and other personal information to make basic background checks possible.

9.017 There should not be restrictions on the videotaping and other surveillance of personnel that would prevent these security measures from being employed effectively inside production facilities.

9.018 The discovery rules in court proceedings should make it possible to prevent the disclosure of trade secrets and other proprietary information, while still allowing enough information access to let a court case go forward without undue handicaps.

The nature of the corporate relationships

General conditions needed to make corporations behave responsibly

9.019 Corporations should be legally required to be truthful in their public accounts, statements, and filings.

9.020 The ownership and control of the corporation should be sufficiently transparent, so that the personal reputations of those responsible for the corporation's policies and activities will suffer if the corporation does not conduct itself properly.

© 2012 Internet Security Alliance

9.021 Corporate officers and senior executives need to be held personally and legally responsible for acts of professional misconduct or negligence while carrying out corporate business.

9.022 The corporation engaging in electronics supply contracts should have enough brand value or other assets at stake, so that its owners would suffer a considerable loss, in proportion to their investment, if the corporation went out of business.

Audit conditions to be included in the supply chain contracts

9.023 The corporate customer needs to have the right to perform security audits of any aspects of production that would not reveal the supplier's trade secrets, business plans, negotiating positions, or other competitively sensitive information.

9.024 In cases where an important security audit *would* reveal the supplier's trade secrets, business plans, negotiating positions, or other competitively sensitive information, the contract should designate a mutually agreed-upon third party to perform the audit.

9.025 Any third parties employed for audits should be contractually held to the strictest security requirement mentioned in the relevant section of these guidelines.

9.026 If the contract is important enough to both the supplier and the corporate customer, arrangements should be made for the corporate customer to have one of its personnel posted in the supplier's production facility as a resident representative.

Financial penalties for security lapses to be specified in the supply chain contracts

9.027 Whenever possible, financial penalties should be contractually agreed upon for failures to comply with contractually specified security measures, similar to the penalties (liquidated damages) that are regularly agreed upon for delivery delays, failure to maintain specified quality levels, and other service shortfalls.

9.028 The financial penalties for security failures should apply regardless of whether the security failure was intentional or whether it resulted in actual damages.

9.029 Some of the security compliance failures that should result in financial penalties include:

- failure to promptly admit inspectors arriving for surprise visits to physical facilities
- failure to provide prompt and full access to computer logs, access records, task assignments, inventories of parts and materials, and other documents required for contractually specified audits
- the purchase of parts from gray market suppliers without appropriate provenance
- failure to adequately control access to the production facility or to the production facility's information system
- failure to account for parts and materials that were supposed to be tracked

9.030 International arbitration boards should be contractually agreed upon for determining whether there has been compliance with the contract, what penalties, if any, should be assessed, and how large these penalties should be, given the specifications in the contract.*

© 2012 Internet Security Alliance

Police and criminal courts

Law enforcement operations

9.031 The police should pursue criminals accused of stealing trade secrets, confidential data, and other intellectual property as energetically as they would pursue criminals accused of other white-collar crimes involving similar losses, such as embezzlement.

9.032 The police should pursue criminals accused of crimes against foreigners and foreign corporations as energetically as they would pursue criminals accused of crime against local citizens and local corporations.

9.033 There should be a regular channel by which senior police officials and international business representatives can get to know each other and through which they can arrange for mutual help with the prevention and investigation of crimes affecting electronics manufacturing.

9.034 The police should be receptive to evidence provided by corporations carrying out their own investigations of criminal activities threatening their operations, and the police should be ready to act on that evidence.

9.035 The police should have training in the proper ways to seize, preserve, and examine digital evidence, so that so that it can be used effectively in legal proceedings.

9.036 The police should have the ability, with proper court approval, to seize, copy, and preserve data stored in computer systems owned by or under the control of organizations and persons suspected of criminal offenses.

9.037 The police should have the ability, with proper court approval, to collect traffic data on electronic communications by organizations and persons suspected of criminal offenses and, if appropriate, to intercept, record, and preserve the content of those communications.

9.038 The police should co-operate with international investigations into crimes affecting the production of electronics components and products, including the theft of trade secrets or confidential data, infringement of copyright, and counterfeiting of electronic components and products.

9.039 Judicial officers and prosecutors should be trained in the proper introduction and examination of digital evidence during legal proceedings.

Criminal penalties that need to be applied

9.040 Organizations and persons convicted of criminal acts, such as theft of trade secrets or confidential data, infringement of copyright, counterfeiting, and misrepresentation of items offered for sale, should be required to provide restitution for the damages caused by those criminal acts.

9.041 The courts should recognize that in some cases, a partially suspended sentence and term of probation might be appropriate to enable the organization or person in question to provide greater restitution to those harmed by the crime.

9.042 Organizations and persons convicted of criminal actions, in addition to providing restitution, should be made to suffer a penalty great enough to deter any similar crime. This means that the penalty should be significantly greater than the gains an offender could expect to make from similar crimes before being caught and prosecuted.

© 2012 Internet Security Alliance

9.043 In determining the size of the penalty necessary for deterrence, the scale of the crime should be taken into account, including the amount the organization or person intended to gain by the crime, the amount of damage the organization or person was willing to cause in the commission of the crime, the extent to which the organization or person appears to have habitually pursued or tolerated criminal activity, and the degree to which the organization or person obstructed (or facilitated) the investigation of the crime.

9.044 Remedies should be routinely imposed that limit the continuing harm that could result from the offense and that prevent repetition of the offense.

9.045 Special consideration should be given to any remedies requested by the injured parties.

9.046 Organizations that exist primarily for criminal purposes, if convicted, should be required to pay fines that deprive them of all their assets.

9.047 Serious or repeat offenders found guilty of large thefts of trade secrets, confidential data, or other intellectual property should be eligible for prison terms.

9.048 Serious or repeat offenders found guilty of large scale counterfeiting of electronic components or devices should be eligible for prison terms.

Expert Contributors to This Project

The names in boldface are those who contributed to the final series of workshops and discussions that directly provided material for the drafting of these guidelines. The other names are those who contributed their expertise to the workshops held during earlier phases of this project. The organizational affiliations listed for the contributors are the ones that were current at the time of their participation. *The participation of experts affiliated with these corporations, governmental bodies, and other institutions should not be interpreted as an official endorsement of these guidelines by those organizations.* These experts are listed here to acknowledge the many hours of advice and discussion that most of them contributed to this project and to indicate the range of viewpoints and professional experiences that went into the creation of this document.

Robert Abrams (NJVC)

Mike Ahmadi (GraniteKey)

Nick Akerman (Dorsey & Whitney)

Christina Ayiotis (CSC)

Nadya Bartol (Booz Allen)

Drew Bartkiewicz (Hartford)

Patrica Becker (Northrop Grumman)

Jennifer Bisceglie (Interos)

Joerg Borchert (Infineon)

Stan Borgia (DoE)

Jon Boyens (NIST)

Matt Broda (Nortel)

John Bumgarner (US-CCU)

Brian Callahan (Boeing)

Jeff Carlisle (Lenovo)

John Carter (NSA)

Matt Carpenter (InGuardians)

Thomas Calderwood (Oracle)

Daniel Chen (Mitsubishi)

Larry Clinton (ISA)

Brian Cohen (IDA)

Al Cook (IBSS)

Guy Copeland (CSC)

Jack Danahy (Ounce Labs)

Don Davidson (DoD)

Paul Davis (NJVC)

Thomas Dillon (DoD)

Lawrence Dobranski (Nortel)

David Doughty (Intel)

© 2012 Internet Security Alliance

Mark Duesenberg (Lenovo)

Hossam Elddin Saleem (Universal Motors Agencies)

Kevin Engfer (Northrop Grumman)

Mark Esherick (Siemens)

Jack Farris (Verizon)

Severio Fazzari (Booz Allen)

Vance Fields (Northrop Grumman)

Mohan Ganesan (Satyam Computer Services)

Michael Greelish (Northrop Grumman)

Jeff Givney (Lockheed Martin)

Marc Goodman (Cyber-crime Research Institute)

Werner Gutau (Infineon)

Meg Hardon (Infineon)

Pete Hartigan (Trusted Ventures)

Mike Hickey (Verizon)

James Hoe (CMU)

David Hoffman (Intel)

Richard Howard (iDefense)

Thomas Indelicarto (VeriSign)

Grant Jewell (Northrop Grumman)

Sue Graham Johnston (Oracle)

Stewart Katzke (NIST)

Mike Kennedy (Motorola)

David Lang (Dell)

Thresa Lang (Dell)

Alan Lawrence (Cisco)

Annabelle Lee (NIST)

Karl Levitt (National Science Foundation)

Joshua Magri (ISA)

Tom Mahlik (FBI)

Scott Mansfield (Ericsson)

Richard Marshall (DHS)

John Miller (Intel)

Rama Moorthy (IDA)

Nick Multari (Boeing)

John Nagengast (AT&T)

Michael Nash (IDA)

Fiona Pattinson (Atsec)

Thomas Patton (Philips Electronics)

Felipe Paez (Dell)

Gary Phillips (Symantec)

Al Piesco (Lockheed Martin)

Michelle Pinto (Harris)

Sydney Pope (DoD)

Andy Purdy (CSC)

Michael Purdy (Dell)

Cindy Reese (Sun Microsystems, Oracle)

Hart Rossman (SAIC)

Warren Russell (DoD)

Marcus Sachs (Verizon)

Rasoul Safavian (Bechtel Communications)

Tony Sagar (NSA)

Bill Scherlis (CMU)

Mark R. Schiller (HP)

Vishant Shah (DHS)

Stephanie Shankle (Booz Allen)

Ken Silva (Verisign)

Matt Smith (NetApp)

Ken Speck (NSA)

Ken Steinberg (Savant)

Marianne Swanson (NIST)

Andras Szakal (IBM)

Bob Thibadeau (Seagate)

Debbie Turnbull (IBM)

Jun Ueda (Renesas)

Ray Williams (L-3 Communications)

Ben Winter (Lockheed Martin)

© 2012 Internet Security Alliance

A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels

Jeff Brown, CISO, Raytheon Company

In today's cyber security environment there is one inescapable truth. There is no way to prevent a determined intruder from getting into a network so long as one allows e-mail and web surfing –and no business today can long survive without these two bedrocks of the information age.

The reasons for this are simple. The vast majority of our Information Assurance architectures rely on patching and configuration control for protection, the consistent application of which has thus far proven elusive over large enterprises. It also relies on signatures for both protection and detection which, by definition, will not stop the first wave of the increasing volume of zero day attacks we are seeing today. Therefore, when you must let the attack vector (an e-mail or a web address) past your perimeter to the desktop, you are virtually guaranteed to have successful penetrations.

Raytheon believes the best way to address this new reality is to recognize that attackers will get into your network and expand our defensive actions to detect, disrupt, and deny attacker's command and control (C2) communications back out to the network. It is an acknowledgement of the fact that there are fewer, or perhaps relatively noisier, ways to get out of a network than to get into it. Such a strategy focuses on identifying the web sites and IP addresses that attackers use to communicate with malicious code already infiltrated onto our computers. While some of these sites are legitimate sites which have been compromised, the majority are usually new domains registered by attackers solely for the purposes of command and control. There is little danger of unintended consequences from blocking these web sites and their associated IP addresses for outbound traffic. Where they are legitimate sites, the benefit of protecting the enterprise far outweighs any inconvenience there might be if an employee needs to legitimately go to that site. Raytheon has had success with this strategy, but it requires a significant investment, unaffordable to most small and medium size entities and many larger ones.

One of the corollaries of recognizing that networks can always be penetrated is a shift in how we measure ourselves. Measuring ourselves against how many intrusions occur becomes a far less interesting. What counts, instead is the intruder's dwell time in our network, or how long an intruder has had access. It's more important to recognize how successful the penetrations were versus how many penetrations occurred. The ideal goal would be to have

advance notice of a new malicious C2 channel so that even if someone opened a malicious e-mail the outbound C2 channel would already be blocked—making the effective dwell time zero.

There are two ways to reduce the dwell time of an intruder, both of which we are pursuing in Raytheon. The first is to make a considerable investment in traffic analysis and analytical methods to detect the malicious outbound traffic in a network. We have had considerable success in this arena but it has required a large investment that a majority of organizations are not likely to match.

However, the other way to reduce dwell time is a method every organization, large and small, can match--collaboration with other operational entities. If we can take advantage of the good work of other organizations, we are eager to do so. We recognize that many other organizations regularly find and report C2 channels. Anti-virus vendors, CERT CC, managed security service providers, defense contractors, research institutions, intelligence agencies, other large government agencies, and law enforcement all see relatively narrow aspects of the C2 environment. But put them all together and they collectively see a very wide swath of the C2 threat environment. Many already aggregate and share the information formally or informally through ISACs, the Defense Industrial Base Cyber Task Force, Infraguard, or any number of other forums. But there is no central clearing house for this information or an operationally focused framework for rapid dissemination of this threat information to a broad national audience.

It is in the collaboration realm that Raytheon believes there is an opportunity for a national scale effort that can turn collective effort to our advantage in the cyber battle. The gaping hole in cyber collaboration (often called information sharing) is that the vast majority of small and medium–sized organizations, both commercial and government, do not participate in these groups or do not have the resources to take advantage of this information when they get it. Unfortunately, for many in critical infrastructure sectors, these small and medium-sized organizations represent a significant portion of our supply chain. We have a vested interest in their success.

While there is no national-scale framework in place, there is a model that has already proven effective fighting other cyber security problems. The model involves a set of trusted entities developing threat information and reporting voluntarily (with non-attribution) to a central source, which consolidates the information and rapidly disseminates it to a very large user community. The user communities, in return, implicitly trust the centralized service and expend little or no resources to validate the information. They simply let the automated processes protect them as a passive service rather than investing in active collaboration—and with much better results.

If this sounds familiar, it's because it is the model used for the highly successful anti-virus and spam filtering industries. We propose that this same model be used to disseminate information on attacker C2 URLs and IP addresses and automatically block outbound traffic to them. If attackers get into your network but cannot get back out the attack is effectively thwarted.

Such a model will have a tremendous impact against botnets and the advanced persistent threat both of whom make heavy use of web-based command and control. While the first wave of their attacks might initially succeed they would be short-lived after the first discovery because of the rapid and automated dissemination of the C2 channels. Subsequent waves would fail completely by virtue of rapid dissemination and automatic blocking of the C2 mechanisms. Of course, one could argue that an attacker could always rapidly change their command and control channels and make them unique to each attack. While this is true, the more we force intruders into greater costs and complexity, the more likely we are to change his cost-benefit calculations. It seems axiomatic that anything that is both simple and inexpensive while forcing this behavior is worth doing on our part.

This document, then, proposes a model for standing up a National Cyber Threat Protection Service to implement a C2 disruption strategy. It will describe the process, key relationships, and responsibilities of the participants and the incentives for each community of interest. This is a voluntary model. Within all the communities described below, not everyone has to participate for the model to be effective. The more the better, but once the process includes a critical mass, the benefits will quickly accrue to a wide swath of both the public and private sector.

An Industry-Government Cooperative Model for Disrupting Malicious Cyber Command and Control.

There are three types of entities involved in this process:

1. **Threat reporters** discover and report malicious C2 channels.
2. **A National Cyber Threat Response Center (NCTRC)** which acts as a central threat clearing house, collecting the threat reports, vetting them as necessary, and providing them to vendors in a standard format.
3. **Vendors for firewall devices** (the term here being used in its most generic sense) would accept the new threat information and push it out to their devices in the field the same way anti-virus and spam filtering vendors push new definitions today.

Certified Threat Reporters.

Threat Reporters are organizations with the detection and analytical capability to discover command and control sites via malware reverse engineering or traffic analysis. Organizations, be they commercial, private, or governmental, would apply to be certified as Threat Reporters and have their reports of C2 channels accepted as valid.

Some third party, presumably a government entity, an industry consortium or some hybrid of the two, would be responsible for certifying potential Threat Reporters against a moderate standard of in-house capabilities. The standard would measure both quality and quantity. Quality would be evaluated by a review of in-house detection and analytical capabilities designed to give *a priori* confidence in their reports' reliability. This would ensure the information the reporters provide is credible and allow for a more rapid automated dissemination process with minimum manual review. Quantity would be measured after certification to ensure the reporter was contributing enough unique threat information to the community to continue to merit the marketing advantage of being a Certified Threat Reporter.

It is important to note that submission of reports by Threat Reporters would not be the same as disclosing breaches required under other laws or agreements. A significant percentage of reports would come from intelligence or other detection activities not associated with any activity within the reporting organization's network. For this model to be viable the reporters have to be free to provide threat information without any implication that they experienced a breach or might get requests for involuntary disclosure of additional information.

Threat reporters would normally submit only malware command and control information, either web sites or IP addresses and the class of threat (e.g. botnet, advanced persistent threat, etc). That information, alone, is enough to make this model work if all parties trust the credibility of the assessment. Other detailed information on the malware involved could be voluntarily submitted, but not at the expense of rapid submission of the C2 channels.

The advantage to the Threat Reporters, especially managed security service providers, is in their ability to use the certification for branding purposes. Organizations that develop threat data internally but which do not wish to participate due to low risk tolerance or because they feel reporting might conflict with their business model would simply not apply to become Threat Reporters.

National Cyber Threat Response Center (NCTRC)

The role of the NCTRC is to serve as a clearing house for processing reports of C2 URLs and IP addresses from Threat Reporters and rapidly distributing them to the community of firewall device vendors. By having a central point disseminating the information to all vendors equally we avoid the problem we face with anti-virus today where not all vendors detect all threats. The NCTRC would also deconflict erroneous reporting that resulted in disruption to

legitimate activities. The NCTRC would maintain a "reputation index" (e.g. credibility rating) for each reporter much like seller ratings on eBay. By this feedback loop a Threat Reporter could be decertified (i.e. no longer have their reports accepted or be able to claim Threat Reporter status in their marketing).

The NCTRC must be a single organization focused on rapid dissemination of actionable information. Unlike the current anti-virus business model where organizations submit malware to their vendor of choice, there would be only one clearing house. The question of who operates the clearing house is largely irrelevant so long as everyone in the model trusts them. It could be a government entity or, more likely, a non-profit organization overseen jointly by the government and an industry consortium. Regardless of who operates the NCTRC, the government must be as secure reporting information to it as industry is. With the large amount of IP threat information the government sees simply because of the size of its network, the absence of threats detected in their networks would significantly reduce the value of the model.

Firewall Device Vendors

Producers of devices that are capable of blocking outbound web traffic would accept the data from the Clearing House, reformat it as appropriate for their device, and push it out to their customers as quickly as possible. Traditional desktop or network firewalls, web proxies, and routers would all be capable of performing this function, thus giving network owners a wide variety of products from which to select based on their architecture and investment tolerance. The vendors would differentiate themselves from each other not only on price, but also on their speed of updates and value-add services such as the ability of their customers to manually override the lists or their ability to provide reports to network owners.

Industry, Critical Infrastructure Providers, and Government

The real benefit from this model lies with the vast majority of network owners in business, industry, and government who cannot afford the deep detection and analytical capability needed to protect themselves. Today, these organizations are totally at the mercy of a determined intruder who is virtually guaranteed to be able to compromise systems with socially-engineered zero-day attacks. Most simply do not have the investment dollars to build a detection infrastructure dependent on traffic analysis or the expertise to make use of the various information sharing groups. With this model, though, these businesses could easily, and voluntarily, afford a single device that most already have anyway.

It would, however, now provide an order of magnitude increase in the level of protection by stopping in near-real time many of paths an attacker would use to get back out of the network. For those who had not been compromised yet when updates come out, they

would completely nullify any subsequent attack with that command and control channel. For those who had already been compromised in the first wave of a zero day attack, it would minimize the length of time when an attacker could access the compromised box and it would identify compromised computers that might otherwise have gone undetected. Best of all, assuming they implicitly trust the system, the organizations employing the model do not have to invest any additional resources to take full advantage of the model.

A secondary benefit would accrue to organizations whose websites have been hijacked and used as C2 sites (as opposed to dummy domains registered specifically for C2). These organizations would become aware of the infection more quickly as hits on their web sites dwindled or simply monitoring the NCTRC lists. They would be then able to exhibit good internet citizenship by quickly cleaning their systems and working with the NCTRC to be removed from the block list.

A third benefit, although perhaps more appropriate to a follow-on effort, would be the ability to tie the reported C2 channels to a library of instructions for finding and cleaning the specific malware where is was detected. This would be a much more complex and less automated process, but it would give smaller organizations a quick way to not only know they have a problem, but also allow them to short circuit the remediation process.

The Prospect of a Common Operational Picture

Perhaps one of the most tantalizing side benefits of this model is that it could be the basis of a true Common Operational Picture. If every firewall device supporting this model not only blocked the outbound traffic, but also—again, voluntarily—reported back to the Clearing House that there was a blocked C2 attempt from their IP address it would, given the potentially hundreds of thousands of devices reporting in, represent a very accurate picture of the scope of any given attack or campaign. Unlike today when organizations are loathe to report incidents because of the risk of bad publicity, data reported to this COP would not reveal any information beyond the fact that someone on their network tried to communicate with a bad URL or IP. Plus, by definition, if the firewall device blocked the outbound traffic, the attack failed or has been neutralized. But knowing the nationwide scope of attacks from the same source would yield invaluable information unavailable today.

If the IP addresses reporting in could be grouped by their critical infrastructure or agency, the COP could be filtered to that organization. For example, if the NCC knew the IP space of all nuclear power plants, a COP could show attempts to access the same C2 sites from multiple power plants. This might indicate a concerted effort to compromise the plants.

Similarly, the defense industry or financial community would see the scope of attacks across their community. Or the Department of Defense would see which attacks were unique to them since there might be no detections of specific C2 sites outside of DoD IP space. And all this in near-real time.

Incentives

This model for denying and disrupting attacker command and control on a national scale includes positive incentives for every participant.

1. Organizations, especially commercial entities, will have an incentive to be certified threat reporters for branding purposes. It shows that they have a robust, capable process and investments to become credible reporters of threat data. There could even be tiered levels for branding purposes based on the volume and accuracy of inputs, i.e. an anti-virus vendor who might report a lot of C2 URLs based on all the malware they get would be Platinum Reporters. A large company with robust internal capabilities might be a Gold level. Managed Security Service providers would be especially eager to participate since the number of C2 channels first reported by them would be a tremendous marketing tool.
2. The Government will greatly benefit by being provided a very large body of C2 URLs and IPs with very little investment on their part. They will also benefit, of course, by the overall increased security of the industrial base which is a major goal of US policy. Most important, however, is the promise of a near-real time common operating picture that truly reflects the current threat environment. The main burden on the government's part would be the up front effort to champion implementation and develop interface standards for receiving reports and disseminating them to vendors.
3. Firewall device vendors will have a great incentive to participate. They will be noticeable by their absence if they don't participate and it will most likely open up a whole new class of customers who see in a single device a high payoff defensive measure.
4. Best of all, small and medium sized organizations of all types will now have a way to take collective advantage of the investigative work of the best IA organizations in the country. By investing only in the firewall device that best fits their architecture, their security will increase by an order of magnitude or more simply because, like AV, a known bad domain will get blocked within hours of discovery.
5. This would also help to restore trust in the internet by identifying and isolating ISPs that do not maintain standards of good behavior on their networks. Their IP space and registered domains would frequently be blocked, presumably reducing their profitability and providing an incentive to good behavior.

6. Once this model is up and running it could easily be extended internationally. In fact many foreign producers would have a great incentive to have their devices capable of participating in this model. From there it is a short jump to an international model.

Risks

The main risk associated with this model is the risk of blocking a legitimate web site that has been taken over by an attacker for use as a Command and Control site or downloader site. While we believe this risk will be small compared to the gain, the model envisions a reclama or deconfliction process whereby a domain owner could get his domain removed from the list either as an error or after demonstrating his site was no longer hijacked. A secondary mitigation would be for the vendors to allow manual overrides on blocked domains at the local level, exactly as is done today with exceptions to web proxy vendors' predefined categories.

There is a secondary risk involved in building the trust relationships required to make this model work. Industry and government alike must be assured that there is no negative connotation to submitting threat data. The simple imperative of getting malware command and control data out to the broadest possible audience must take precedence.

Summary

This model, if implemented on a national scale, has the potential to be a game changer. For every attack, if a single organization discovered the attack, the entire nation would soon be protected. It would force an attacker to make the command and control channel unique for every attacked IP address. An attacker would have to either reduce the scope of attacks or greatly expand his domain registrations. In the later case, someone registering enough domains to operate on the level our attackers operate today would soon gain such a high profile they would be susceptible to other mitigations.

In the end, this model takes the best aspects of today's anti-virus, spam filtering, and proxy URL categorization to build a fourth service that is akin to anti-virus on outbound traffic. This National Model for Disrupting Attacker Command and Control proposed in this paper could set a new standard for effective public-private partnership in the Internet Age.

March 23, 2012

The Honorable Greg Walden, Chairman
House Energy and Commerce Committee
Subcommittee on Communications and Technology
2182 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden,

I am pleased to submit McAfee's responses to the questions following your Subcommittee's hearing on *Cybersecurity: Threats to Communications Networks and Private-Sector Responses.*

Please feel free to call on me for any other information you or the Subcommittee might need, and thank you for requesting McAfee's views.

Sincerely,

Dr. Phyllis Schneck
Vice President and Chief Technology Officer, Public Sector
McAfee, Inc.

From The Honorable Greg Walden

1. **Mr. Lewis mentioned in his written testimony that the government could play a coordinating and incentivizing role regarding the widespread adoption of Security Extensions for the Domain Name System, also known as DNSSEC. Do you agree, and if so, what should the government do specifically?**

Government has a strong role to play in cyber security to enable the use of better technology and further innovation through financial, tax, or other incentives. We agree with Dr. Lewis on the importance of securing the DNS system and think that incentives would help expedite this process in currently applicable ways now and even stronger technologies in the future.

Incentives would relieve the human and time resource burdens that are often an obstacle in the implementation of cyber security, and additional funds could also spark some creativity within companies by resourcing subject matter experts to explore better implementations or technologies.

In today's business climate, resources are scarce and cyber security often suffers because it is not tangible. Government incentives could free some funds that would be dedicated to augmented cyber security implementation and innovation from DNSSEC and forward.

2. **Mr. Clinton in his testimony mentioned the formation of an "underwriters' laboratory" style information clearinghouse for cyber security. What do you think about that idea? Would sharing additional information with cyber security insurance providers, perhaps through private-sector clearinghouses and with appropriate privacy safeguards, help foster the development of such a program?**

We support the idea of a clearinghouse for cyber information so that data from companies like McAfee could be combined with other relevant data, including from the government. That information – both automated event data and human-perceived data – would be sanitized, including the removal of any personally identifiable information. It would then be extremely useful not only for insurance purposes, but also in warning ISPs so they could electronically block IP addresses from sources known to be malicious.

If, however, an "Underwriters' Laboratory" implies a third party certifying the security products of private sector entities, we would not support the idea. It is one thing for the private sector to agree to adhere to standards or best practices; it is another to have those standards regulated or "approved" by an independent body. We would support the former but not the latter.

3. **Several members of the panel highlighted the need to remove legal impediments that may prevent Internet service providers, cyber security software providers, and others to address cyber threats and share information. Could you identify any specific federal or state laws, regulations, or other legal impediments that Congress can address to improve cyber security?**

There is a complex web of rules that have the effect of creating an environment of disincentives for ISPs and other telecommunications providers to collaborate with security companies in addressing the cyber security challenge. The *Stored Communications Act of 1986* is one example of a law that prevents ISPs from disclosing information about communications outside of their organization.

In addition, there are laws and statutory environments that prevent meaningful information sharing. These include the Freedom of Information Act (FOIA), discovery provisions in general, a lack of immunity for disclosure of information, and no limitation of liability.

For instance, imposing limitations on liability for damages as well as for non-economic losses would remove a serious obstacle to information security

investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company's good faith investments in adequate information security. Eliminating that risk, at least for companies that meet high, "best practices" security standards, would encourage more security on a company-by-company basis. This approach could help create positive incentives for disclosure through liability relief for responsible organizations to improve the nation's overall cyber security posture.

We re-emphasize the point that telecommunications providers often have a very comprehensive threat picture. If they could combine that "radar map" with others, then the ability to detect and respond to cyber threats would be augmented. We need to share more and better information than our adversaries in order to have the more complete snapshot of network activity to detect and prevent harm.

4. I have seen reports that indicate that many cyber security breaches could be avoided if businesses followed best practices. What are some of these techniques and how can we encourage more companies to adopt them?

Good cyber hygiene is certainly a good starting point and can prevent many – though not the most pernicious – cyber attacks. Any organization, government agency or individual can employ basic hygiene techniques such as the following:

- Change the default passwords that are on devices when they are shipped.
- Do not click on/open links from an unknown source.
- Make a conscious decision about how much personal information you want to reveal online.
- Be wary of using a portable drive/thumb drive if you do not know its origin.

More information is available on several sites, including the National Cyber Security Alliance.

There is one large caveat to this advice, however: Even the best hygiene will not stop an Advanced Persistent Threat (APT), which is an insidious intruder that flies below the radar. An APT is a cleverly designed and targeted instruction set that maintains its "persistence" via remaining quiet and uses that "persistence" to gain unauthorized access to data or operations. This type of threat can enter a system no matter what one does, and more aggressive tools are necessary to counter it.

5. The Internet is currently transitioning from IPv4 to IPv6 addressing. Does that process create any new cyber security issues? Will

transitioning to IPv6 alone solve any cyber security issues that currently exist? Does the process of transitioning to IPv6 present opportunities to resolve existing cyber security issues?

The transition from IPv4 to IPv6 is underway, designed to broaden address space. The transition alone will not make things more secure. In fact, it opens up new vulnerabilities, as new configurations will be required in Internet traffic protocols. However, IPv6 also brings new functionality that, if implemented correctly, can, for example, cryptographically protect the identity of addresses of machines on a network.

In the case of IPv4 or v6, IPSEC implementation can add to security, with the ability to maintain a key for cryptographic authentication of traffic.

The message here is the same as with many other parts of technology and the Internet ecosystem. Technology alone will not bring security. A thoughtful, risk-mitigation-based, policy-driven implementation of solid technology is the key to cyber resilience.

6. **In December, we heard from witnesses that the implementation of "WhoIs" databases makes it difficult for companies and law enforcement to identify and track down the owners of websites that are facilitating illegal conduct, including sites that host malware. What is the private sector doing to strengthen the use of WhoIs to help combat cyber criminals, and are there any steps Congress can take to facilitate that work?**

While the WhoIs database might be interesting or useful for the general public, security professionals and law enforcement do not rely on WhoIs for accuracy. We have other resources we use to identify the actual location or owners of traffic and websites that might be compromised. These paid resources are more reliable for our purposes.

From The Honorable Anna Eshoo

1. **Several agencies, including the FCC, have been exploring a voluntary, industry "code of conduct" as a way to address the detection and mitigation of botnets. Do you support such an effort, and how do we ensure it's effective?**

The idea of a voluntary code of conduct for industry was used to good effect in Australia. ISPs agreed to share data and tell their users when they had a compromised machine. Those machines would then not be useful to botnet perpetrators.

A truly voluntary code of conduct makes good sense. Government could create a forum for arriving at the code of conduct and help to drive the process forward, as the FCC has done with CSRIC. We are pleased to see that CSRIC has adopted recommendations for voluntary action by ISPs to combat three cyber security threats, and we are equally pleased that several of the nation's largest ISPs have agreed to implement these measures. The process must remain voluntary, however, or it will not succeed.

2. **For many years, the E-rate program has helped schools and libraries with discounted telecommunications services. As I understand, E-rate discounts are available for basic firewall protection but don't extend to other security services. Has this made our schools and libraries more vulnerable to a cyber attack?**

E-rate is a good program to bring connectivity to schools and libraries. We would suggest augmenting it, however, by ensuring that the connections and machines are secure. Right now, the only cyber security tool that is eligible for the E-rate discount is a firewall. Cyber security has progressed well beyond that, of course, as malware can enter a machine via flash drive, emailed attachments, or websites that may not be caught by a conventional firewall. The end hosts must be protected, and the gateway (firewall) cannot be the only filter.

We do not have full insight into the program, but we suggest that some basic cyber security goals around risk mitigation be spelled out in the requirements. It would be important to focus on the goal and not spell out specific technologies, as these will constantly change.

Indeed, in our experience, schools that build strong security programs leverage a wide array of technology solutions that protect their entire infrastructures from end to end – from the point that their IT infrastructures interconnect to the Internet all the way back to their students. This type of layered security model is an example of best practice that policy should support.

It is quite possible that the recipients of the E-rate discounts already provide robust cyber security. We simply recommend bringing cyber security into focus for the program. That only makes sense, especially given the FCC's emphasis on good cyber security practices.

3. **Your testimony highlighted your company's significant investment in R&D and why additional investment in cyber security research is so important. How can Congress help encourage continued investment in this area?**

Funding cyber security R&D in the United States has many obvious technological advantages. There is another advantage that might not be so obvious, however, and that concerns our global leadership.

The best way to learn something is to do research and work in it. Therefore, providing increased R&D funding would augment the cyber workforce – a matter of great concern for both the private and public sectors. Right now, many researchers at our best universities leave and return to their home countries overseas, leaving the U.S. with a talent drain. If we funded more R&D here, researchers might stay. We also need to update our immigration laws to enable talented foreigners with unique technical skill sets to stay in America and contribute to the growth of our own information technology economy.

The government has several programs that encourage and fund research in cyber security. Some are even targeted at identifying and solving the problem sets considered to be the most "hard problems." We believe that more funding toward these efforts would elevate our national research programs and attract the best minds from all over the world, which would also help drive global standards and innovation.

R&D funding would also create jobs and encourage more people to enter the field of cyber security. This would contribute to our economy and to our technology. All in all, increased funding for R&D would contribute to our global leadership.

From The Honorable Henry Waxman

1. **The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) has been formulating recommendations for best practices to ensure optimal security and reliability of communications systems. How do you see this process contributing to improvements in cyber security?**

The FCC has brought together many in the private sector to look at best practices without taking a regulatory, top-down approach. We are pleased, for example, to see that CSRIC has adopted recommendations for voluntary action by ISPs to combat three cyber security threats, and we are equally pleased that several of the nation's largest ISPs have agreed to implement these measures. We agree with the FCC that voluntary, multi-stakeholder actions exemplified by CSRIC's recommendations, and the corporate commitments to act on them, are one of the most effective approaches to securing our networks while preserving the Internet as an open platform for innovation and communication.

2. **What opportunities do you envision for government and industry to work together towards coming up with critical cyber security solutions? What role specifically do you see for the FCC?**

As my testimony contains several recommendations on how the public and private sector can work together, I will concentrate on just this one recommendation: Establish a process to facilitate real-time information sharing among industry and government players. The process should preserve the privacy of personal information and be independently verifiable. The following paragraphs explain why this mechanism is so critical to stopping cyber attacks.

The data shared could provide real-time situational awareness, comprised of data gathered from machines, as well as correlation and synthesis of such data by human analysts. For example, routers at ISPs can have dynamic malicious IP addresses on their access control lists and can prevent malicious instructions from reaching a target machine. The human-compiled models might show that the malicious activity is taking place in a certain sector, enabling further study by the designated public and private authorities.

Today, traffic sources associated with negative indicators are often admitted into the network fabric without further thought unless they match a known "signature" or unless a network team happens to subscribe to a system such as McAfee's Global Threat Intelligence (GTI). We must extend that watch to include other data sources and put the information out to more networks.

A useful analogy is an immune system: the network can report data and events into a large global set of databases for correlation. The new events that get added enhance the accuracy of the existing data that then go back to protect the network fabric. This would help stop malicious traffic from ever reaching a destination, and simultaneously protect other parts of the network from similar attacks.

The FCC is fulfilling its role well by engaging in many awareness programs. They have an awareness program on cyber hygiene, and they have worked with the Small Business Administration to launch the Cyber Security Small Business Planner – both great initiatives.

In their role as overseer of the telecom industry, they have been collecting industry opinion on issues that matter and looking at areas that need to be studied. For example, they have been collecting views on whether VoIP networks ought to be subject to the same reliability requirements as traditional networks. They are asking good questions about the role of carriers and what might be done differently.

And as discussed above, the FCC is already playing an important role in making it easier to share best practices among industry players. The role they are currently playing, through the CSRIC and other initiatives, is a good one, and we encourage further efforts in a similar direction. What's more, the FCC's resolve to keep any processes it develops voluntary is also an important commitment that should be commended and encouraged.

○