

CYBERSECURITY: NETWORK THREATS AND POLICY CHALLENGES

HEARING BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MAY 1, 2009

Serial No. 111-35



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

U.S. GOVERNMENT PRINTING OFFICE

72-884

WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California
Chairman

JOHN D. DINGELL, Michigan
Chairman Emeritus

EDWARD J. MARKEY, Massachusetts

RICK BOUCHER, Virginia

FRANK PALLONE, Jr., New Jersey

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DEGETTE, Colorado

Vice Chairman

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANE HARMAN, California

TOM ALLEN, Maine

JANICE D. SCHAKOWSKY, Illinois

HILDA L. SOLIS, California

CHARLES A. GONZALEZ, Texas

JAY INSLEE, Washington

TAMMY BALDWIN, Wisconsin

MIKE ROSS, Arkansas

ANTHONY D. WEINER, New York

JIM MATHESON, Utah

G.K. BUTTERFIELD, North Carolina

CHARLIE MELANCON, Louisiana

JOHN BARROW, Georgia

BARON P. HILL, Indiana

DORIS O. MATSUI, California

DONNA M. CHRISTENSEN, Virgin Islands

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

CHRISTOPHER MURPHY, Connecticut

ZACHARY T. SPACE, Ohio

JERRY McNERNEY, California

BETTY SUTTON, Ohio

BRUCE BRALEY, Iowa

PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member

RALPH M. HALL, Texas

FRED UPTON, Michigan

CLIFF STEARNS, Florida

NATHAN DEAL, Georgia

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOHN B. SHADEGG, Arizona

ROY BLUNT, Missouri

STEVE BUYER, Indiana

GEORGE RADANOVICH, California

JOSEPH R. PITTS, Pennsylvania

MARY BONO MACK, California

GREG WALDEN, Oregon

LEE TERRY, Nebraska

MIKE ROGERS, Michigan

SUE WILKINS MYRICK, North Carolina

JOHN SULLIVAN, Oklahoma

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

PHIL GINGREY, Georgia

STEVE SCALISE, Louisiana

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

RICK BOUCHER, Virginia

Chairman

EDWARD J. MARKEY, Massachusetts

BART GORDON, Tennessee

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

BART STUPAK, Michigan

DIANA DeGETTE, Colorado

MICHAEL F. DOYLE, Pennsylvania

JAY INSLEE, Washington

ANTHONY D. WEINER, New York

G.K. BUTTERFIELD, North Carolina

CHARLIE MELANCON, Louisiana

BARON P. HILL, Indiana

DORIS O. MATSUI, California

DONNA M. CHRISTENSEN, Virgin Islands

KATHY CASTOR, Florida

CHRISTOPHER S. MURPHY, Connecticut

ZACHARY T. SPACE, Ohio

JERRY McNERNEY, California

PETER WELCH, Vermont

JOHN D. DINGELL, Michigan (ex officio)

FRED UPTON, Michigan

Ranking Member

J. DENNIS HASTERT, Illinois

CLIFF STEARNS, Florida

NATHAN DEAL, Georgia

BARBARA CUBIN, Wyoming

JOHN SHIMKUS, Illinois

HEATHER WILSON, New Mexico

CHARLES W. "CHIP" PICKERING,

Mississippi

VITO FOSELLA, New York

GEORGE RADANOVICH, California

MARY BONO MACK, California

GREG WALDEN, Oregon

LEE TERRY, Nebraska

MIKE FERGUSON, New Jersey

CONTENTS

	Page
Hon. Anthony D. Weiner, a Representative in Congress from the State of New York, opening statement	1
WITNESSES	
Dan Kaminsky, Director of Penetration Testing, IOActive	3
Prepared statement	6
Rodney L. Joffe, Senior Vice President and Senior Technologist, NeuStar	12
Prepared statement	16
Larry Clinton, President and CEO, Internet Security Alliance	23
Prepared statement	26
Greg Nojeim, Senior Counsel, Center for Democracy and Technology	42
Prepared statement	44

CYBERSECURITY: NETWORK THREATS AND POLICY CHALLENGES

FRIDAY, MAY 1, 2009

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

The subcommittee met, pursuant to notice, at 1:04 p.m., in Room 2123, Rayburn House Office Building, Hon. Anthony D. Weiner presiding.

Present: Representative Weiner.

Staff Present: Amy Levine, Senior Counsel; Greg Guice, Counsel; Sarah Fisher, Special Assistant; Amy Bender, Minority Counsel; Neil Fried, Minority Senior Counsel; and Sam Costello, Minority Assistant.

OPENING STATEMENT OF HON. ANTHONY D. WEINER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. WEINER. Welcome to the hearing of the Energy and Commerce Subcommittee on Communications, Technology, and the Internet.

I welcome the witnesses.

Since April 17th, President Obama has had on his desk recommendations of a panel that has been studying cybersecurity policies and structures of our government. Already we have heard a push and pull going on behind the scenes and increasingly in public about some of the thorniest questions that that panel will consider.

Today we will offer some advice.

This committee will have the jurisdiction to implement the policies that are recommended by the President, and notwithstanding the activities in some other committees, which we welcome, the jurisdiction for these matters will be here in the Telecommunications Subcommittee and in the Energy and Commerce Committee.

We will hear from a brilliant set of witnesses, but we will not hear from someone from the administration for some reasons obvious and some reasons not so. The obvious is I don't think they know what their policies will be. So asking them to testify on them might be premature. But also we wanted to, by design, to have a conversation here among interested parties in the community that would allow us to inform our reactions to the administration's proposals that will be forthcoming.

In fact, cybersecurity is not a singular problem. It is at least three. There are, of course, the issues of personal security, issues of spam and nuisance, but also identity theft and the like. This is also an issue of critical infrastructure and protecting it, the economic security of our country and, frankly, the increasingly interconnected economies of all of the countries of the world.

And of course, this is a national security issue. An issue that has been seemingly increasingly brought to the public's attention with stories that fill up the newspapers on everything from fighter jet plans being stolen to Chinese-based spying on Tibet and some of the other countries. We have heard just about a story a day.

We will endeavor to ask and answer some of the big questions that the President is going to be wrestling with. How do we respond to or mitigate or work around or generally respond to the inherent paradox that is the Internet? Its openness, its openness to innovation, its openness to democratization; but also its openness to mischief and mischief makers and often things worse than mischief.

For the most part, Congress has been wise in resisting the temptation for heavy-handed intervention, and that has served the Internet well and has served our country well.

We also have to ask the question that has been dominating the discussions at the White House. Who should be in charge of combating the mischief maker, the con artists or the terrorists; not only what agency of government but whether or not it should be government at all, and if so, what relationship between government and the private sector? With government, of course, you often get the inevitable heavy-handedness and secrecy, but you do get strong centralized action when it is needed. With the private sector you get entrepreneurship, creativity but you also get silos of self-interest that don't always make for vigorous system-wide defense.

One thing is sure. This cancer can't be exorcised with a rusty axe; we need to use a scalpel.

Third, we have to ask the questions, are we destined to constantly fight the last war when it comes to cybersecurity? Is the cycle of discovery, warning, insulation inevitable?

Conficker gave us an interesting and good example of this. Tiffany and my staff put together a timeline of the Conficker virus, and here is what she wrote.

On December 29, 2008 Conficker.B is first detected; Conficker.A updates itself to Conficker.B.

February 20, 2009, Conficker.C is discovered; Conficker.B updates itself to Conficker.C.

March 4th, Conficker.D is discovered; Conficker.C updates itself to Conficker.D.

April 7, 2009, Conficker.E is discovered; Conficker.D updates itself to Conficker.E.

Conficker.E downloads scareware and spyware onto computers. It deletes automatic updates of computer systems and prompts a fake need to update one's computer. And when individuals buy the software protection Conficker.E offers, the computer downloads spyware onto the computer. This is a dynamic that clearly does not lend itself very well to discovering the problem, addressing the problem, moving on to the next problem.

Maybe cat and mouse is our only option. Maybe, though, we don't need a military-type approach but more an approach that we in government use at say NIH or the Food and Drug Administration, where government helps to augment creative solutions, help with some of the R&D, and then let the private sector go off and implement them.

And then, of course, there are the more provocative questions that we might not have time to touch on today, such as John Markoff in the New York Times asking the question, do we need a new Internet all together? Or the provocative title of Jonathan Zittrain's great book, "The Future of the Internet and How to Stop It."

The witnesses we have before us will offer us an opportunity to answer some but not all of these questions. This is a conversation that inevitably has to take place not only here in Congress but in the businesses around the Internet and in the coffee shops and parlors of people's personal experiences and, of course, over at the White House.

Now it is my honor to introduce the witnesses we have before us today.

STATEMENTS OF DAN KAMINSKY, DIRECTOR OF PENETRATION TESTING, IOACTIVE; RODNEY L. JOFFE, SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST, NEUSTAR; LARRY CLINTON, PRESIDENT AND CEO, INTERNET SECURITY ALLIANCE; AND GREG NOJEIM, SENIOR COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. WEINER. Dan Kaminsky is the director of penetration testing at IOActive, where he focuses on design capabilities and vulnerabilities of network protocols. He is probably most famous for having discovered a fundamental flaw in the Domain Name System or DNS that would allow him to reassign Web addresses, take over banking sites, or disrupt the flow of data over the Internet. Thankfully, he was a good hacker and brought this flaw to the attention of those entities that were in a position to fix it.

Dan Kaminsky, you are our first witness.

You are recognized for 5 minutes. I know you have presented some testimony already, so feel free to summarize as you see as appropriate.

STATEMENT OF DAN KAMINSKY

Mr. KAMINSKY. Thank you very much. Hello, everyone. Members of the subcommittee, please allow me to express my appreciation for offering me this opportunity to testify today.

I am, as said, the director of penetration testing at IOActive. I spent the last 10 years of my career working for Fortune 500 companies, including Cisco, Avaya, and Microsoft to help secure their systems.

It was an interesting experience fixing DNS, working with all the people that needed to be in a position to actually get the fix out, get the fix deployed and ultimately protect the ecosystem. It was an example of a public-private partnership. We worked with USCERT in order to get communication out to the Federal agencies that themselves had to get software out. And it was a remarkable,

remarkable experience for all parties. It was a highlight of 2008; 2008 was not, however, an easy year.

Verizon business actually every year puts out a report called the Data Breach Investigation Report. In an industry that always struggles to have good data to work with, Verizon actually did a wonderful thing and has for the last few years in summarizing what they see in their limited sample of their customers base. And what they saw was astonishing. Over 285 million records were compromised last year, just from their customer base. According to Verizon, this is more than every other year they had seen combined. Worse, over 91 percent of those compromised records, most of which were payment card information, over 91 percent of those were traced going back to organized crime.

We have worldwide problems, and we live in a much more dangerous world than when I first started doing computer security years ago. The reality is, hacking is no longer about kids. It is about people with kids who would like to feed them. Attackers have had years to figure out the absolute best ways that they can monetize their access. Recently, they actually managed to coordinate a widespread attack against the ATM infrastructure in which, in 49 cities, \$9 million was extracted from ATMs using purloined ATM data.

Beyond that, extortion, something we have almost no information on, is rumored to be becoming an extraordinary problem not merely hitting the sides or gambling or pornography aspects of the economy but actually standard businesses.

As you mentioned, Conficker. Conficker, it turns out, was a remarkable success. If Conficker had come out in 2003, pretty much every single computer on the Internet, at least every Windows machine, would have been compromised. Since 2003, Windows has become a much, much more secure platform. The actual result of the work from 2003 was probably over 99 percent of the machines that otherwise would have been affected, infected by Conficker never had a problem. That is what happened when we—that is the result of our scans and our monitoring of the situation.

That being said, a percentage of a large number is still a large number, and we have had to deal with millions and millions of machines infected. What was most scary about Conficker is, thus far, we still have no idea what the authors of it want.

So where do most of these compromises come from? How is this happening? A lot of problems are in software. This is true. There is a lot of buggy software out there. But according to the Verizon business report, over 60 percent of actual penetrations that led to loss of data did not come from buggy code; they came from our simple inability to strongly authenticate other nodes on the Internet, default passwords, lack of passwords, lack of insufficiently strong passwords. It turns out authentication is in huge amounts of trouble on the Internet today, and the data suggests it is leading directly to compromises of personal information.

Now people may say, why are we still using passwords? Why is this problem still there? It turns out it is because it is the only way to reasonably make things work at all. It turns out, if something doesn't work, people won't use it, even if it is theoretically more secure.

This is ultimately why I become a supporter of the technology known as DNSSEC. DNSSEC on its face is a method to fix DNS, but it is not just that. DNSSEC ultimately allows us to use DNS's power for allowing communication across organizational lines, ultimately trust across organizational lines, and allows us to apply cryptographic strength to that trust so it can be used not just for existing systems or not just for locating systems but for actually authenticating them and ultimately authenticating the people on the other side. It will take some work. It will take a lot of work, but I see it as the key towards making a new security authenticating ecosystem.

Thank you.

[The prepared statement of Mr. Kaminsky follows:]

Dan Kaminsky
Testimony before the House Subcommittee on Communications, Technology, and the Internet
1-May-2009

===

Members of the Subcommittee, please allow me to express my sincere gratitude for inviting me to speak today about the challenges we face securing the Internet. My name is Dan Kaminsky. I am the Director of Penetration Testing for IOActive, a Seattle-based Security Consultancy, and I have spent the last ten years working with Fortune 500 companies such as Cisco, Avaya, and Microsoft to secure their operations. My particular specialty is in the analysis of large scale systems, and the design faults that they tend to possess. I am best known for my discovery last year of a critical flaw in the Internet's core infrastructure that dated back to 1983. If not addressed, the flaw in the Domain Name System, or DNS, would have exposed almost every website, email, and online account to attackers all over the world. In response, we began a secret collaboration involving every major technology vendor in a position to fix the problem, spawning what may have been the largest synchronized repair event in the history of the Internet.

The DNS patching operation was a success, but 2008 as a whole was a rough year, as that was the year that the monetization of cybercrime really hit. Verizon Business every year puts out a report called the Data Breach Investigations Report, in which they summarize the nature of the data breaches they're hired in to investigate. It has been a rough year. Just in Verizon's customer base alone, they saw 285 million records compromised, the vast majority of which related to payment systems. This is actually more than Verizon saw in the previous four years *combined*. Worse, the percentage of records that could be traced into the hands of organized crime was a full 91%.

This is a worldwide problem, of course. Back in December, journalists with WirtschaftsWoche, or Economic Week magazine, decided to explore what banking records were available on the black market. They found they had the opportunity to, at a cost of little more than half a euro a piece, purchase the banking records of 21 million German bank accounts.

There are only 82 million Germans.

And so we live in the future. Hacking is no longer about kids. It's about people with kids, who would like to feed them. Attackers have had years to hone the best ways to monetize the ever increasing amount of access they're finding themselves with. They are attacking the credit card and ATM infrastructure -- astonishingly, coordinating a worldwide network of so-called "cashers" in 49 cities to extract \$9M in hard currency from RBS WorldPay ATM's, in only 30 minutes. They are acquiring highly sensitive intellectual property -- in a recent example, extracting terabytes of design data regarding the Joint Strike Fighter for purposes unknown. By all accounts, mostly whispers, extortion is becoming an increasing problem -- not just for so-called fringe entities like pornography sites and online gambling operations, but established legitimate businesses as well. A relatively simple but difficult to stop flood of traffic comes in, and a site operator has a choice: Pay up, or lose business.

People pay. We don't have much solid data on who, or how, though. A lack of solid comprehensive data is unfortunately something of a theme in computer security.

And then there are situations where we don't know what the attacker is trying to do. You may have heard about the recent Conficker worm. I am pleased to report that the world did not, in fact, come to an end on April 1st, as some stories may have implied. In fact, Conficker represented something of a coup for Microsoft. Summer of 2003 was not a good time for Microsoft -- to put it simply, Windows was under such constant attack, that it didn't work. Microsoft engaged in a crash program to secure their platform, and six years later, an attack that would have compromised every desktop in the world ended up capturing only a tiny percentage.

Inconveniently, a tiny percentage of a large number is still a large number, and Conficker did infect a few million nodes. Conficker was, and remains special: Not only did it merge the virulent patterns of attacks from 2003 worms with the remote control capabilities of 2008 botnets, it also actively and aggressively defended itself from the security community. We as an industry have been managing the situation, assembling an even larger multivendor effort than was done for the DNS patch. But we don't know who these guys are, and more importantly, we don't know what they want. As my friend and former coworker Jason Larsen, now with the Department of Energy's Idaho labs says, "It's not about ownage. It's about continued ownage." Their game may just be to maintain infection despite our defenses, awaiting further orders. This is not a situation remotely as catastrophic as it might have been. But there are challenges we continue to face, and we have people actively facing them.

So how did we get here? How are attackers causing so much damage? Is it the fact that they feel they can operate with impunity, as law enforcement is based on geography while their operations aren't? Yes, this has an effect. Is it the fact that despite our best efforts, large amount of software exposed to attackers on the Internet remains home grown and insecure, unable to resist the exploits of even a junior attacker? Yes, this is true too, tragically so as while the operating systems have become more secure, the ecosystems built on top of them are struggling. According to Verizon Business, almost 40% of the compromises they see are due to implementation flaws, with a vulnerability known as "SQL Injection" being the second most common vulnerability seen.

What's first?

Default, or shared passwords. There's no "hacking", people just googled the key that's there if nobody changed it, and lo and behold, nobody did! Third is misconfigured access control -- the key opens too many doors. Fourth involves actually stealing a key. Fifth, no key needed after all. Sixth, making a bunch of random keys and seeing if any of them fit. You wouldn't think it'd be this easy, but in 60% of cases, it is.

The keys guarding our castles aren't working very well. So why do we use them? Why don't we get better keys?

Because the better keys don't work that well. All the various devices that are supposed to replace passwords need to be provisioned, managed, replaced when lost, and decommissioned when necessary. The evidence suggests this is difficult, though not impossible when dealing with your own people -- after all, they have badges for doors, don't they? But there is a particular scenario that makes things messy. Quoting the report:

"In approximately four of 10 hacking-related breaches, an attacker gained unauthorized access to the victim via one of the many types of remote access and management software. Rather than for internal usage, most of these connections were provisioned to third parties in order to remotely administer systems."

Too many engineers believe third parties are the exception. They are not. Modern organizations are in fact highly fluid, entering into all varieties of arrangements in which entities

outside the organization need to be strongly authenticated. Right now, that just doesn't happen. You'll generally see a password, but expect it at least to be shared. There's just no reasonable way for one company to monitor and manage who another organization hires. But at least there's some authentication to speak of, because there's a live human involved. The simple reality is, for most communications between hosts, there is no authentication. Clients talk to their Servers, Servers talk to their Databases, Databases talk to their Backups, and with surprising commonality, they never actually check who they're talking to.

That, by the way, was why the DNS vulnerability was so scary. It allowed every and any flow of information on the Internet, and sometimes even on internal networks, to be redirected arbitrarily. Once redirected, even the systems that really, really should have noticed a change...wouldn't.

There is technology that is supposed to fix this. It is called the Global Public Key Infrastructure, and it uses a loose network of approximately 200 companies around the world to assert that I am me and you are you and that each server is allowed to use whatever name it chose. There are approximately one million hosts on the Internet today that are configured to allow some sort of authentication. 40% do not participate in the Certificate Authority system. There is no authentication even tried, just the blind use of encryption. This does not work very well -- if you don't know who you're encrypting to, you might very well be encrypting to the attacker!

Even then, the Global PKI system covers at best 600,000 hosts. In a world of hundreds of millions of systems, that's not much. The Global PKI requires just too many cross-organizational operations to maintain -- and if you try to go without them, to have your own PKI because you don't trust all 200 companies, things get so much more difficult. The Department of Defense has invested heavily in their own private PKI, and has build an authentication platform unrivaled throughout the world. That the Army can know, with a cryptographically authenticated link, that it is communicating with a server with the DNS name of spooky.navy.mil is one of the crowning achievements of information technology.

The US Army locating where on the network spooky.navy.mil is -- determining its IP address -- is by contrast so simple, nobody ever thinks twice about it. It's just a DNS lookup.

Gentleman, I tell you today, these two tasks are practically the same thing. A little bit of information needs to be acquired. It is controlled by someone in another organization. PKI

makes this incredibly difficult. DNS makes it look easy. DNS is a heirarchy -- one root, that doesn't do much. TLD's -- com, uk, mil -- that handle a wide variety of very separate organizations. And so on. It's designed to have a very resilient core, and to need as few interactions between parents and children as possible.

It's worked fantastically. We need more things that work like DNS has for 25 years, and less things that work like PKI has for the last 10.

And so we come to DNSSEC. DNSSEC is not actually that complicated. Normal DNS you get an answer. DNSSEC, you get an answer, and a reason to believe it. There are many people, like Doug Maughan at DHS, who have been carrying the torch of a secure DNS for years. I am not one of them. Some time ago, I decided to really sit down and work with the protocol.

It's actually a good idea. Nobody is more surprised than me.

DNSSEC is interesting not because it fixes DNS, though it does that too. DNSSEC is interesting because it allows us to fix everything else. It's 2009, and we still do not have secure email. This is embarassing! I can send mail easily enough -- DNS tells me what server to actually give the message to -- but I can't make sure that server, or even that user is the only one who can read my message. If only I could securely retrieve an encryption key. Oh -- DNSSEC will let me.

I was in a meeting a few days ago about securing BGP, the protocol the Internet uses to figure out how to actually go about getting traffic from one side of the country to another. The speaker finally started describing how BGP will use certificates, the same sort of system DoD only barely got working at absolutely extraordinary expense and has been a real problem for everyone else. I said to him, this has been blowing up in our face for ten years, why will this be any different? "What else can we try?"

We can try DNSSEC, to allow each ISP to manage their own systems, to express their own trust, in ways they already do today -- in ways we have plenty of evidence can actually work.

Organizational boundaries are hard. DNSSEC makes them not.

From this one base, authentication becomes so much more of a solvable problem. The solution to broken authentication is not to complain louder, to apply more pressure, or even necessarily to deliver more funding. The solution is to change the nature of the system so that it is fundamentally easier, more affordable, and more realistic to solve the problem that needs to be solved. The number of authentication technologies, from secure email to smartcard to systems we can't even imagine yet, that will finally and credibly function to the degree they're needed -- if and only if we can give them a way to bootstrap trust across organizational boundaries -- is tremendous. We can do this. We can make it so much easier to fix a critical weakness, one that is today just leading to lame broken password systems.

We can make it easier for people to do their jobs, to secure their systems, to protect their data.

It will take work, and not just from us geeks. There are political barriers to making this happen. NTIA, over that the Department of Commerce, is working diligently to complete a critical portion of the DNSSEC solution: To "sign the root". It's an unenviable task, rife with international negotiation. I support their efforts here, and I hope you will as well.

In addition, Senators Rockefeller and Snowe have submitted a Cybersecurity Bill in the Senate to begin a comprehensive program to fix the issues we're here to discuss. The bill is still young, and does need some work, but it shows remarkable awareness into the real world problems we have and deserves the attention of everybody here today.

I thank you all for your time and attention.

Mr. WEINER. Thank you.

Our next witness is Rodney Joffe. He is the senior vice president and senior technologist for NeuStar. He is a renowned expert on security flaws in the Internet. He also participated in the Department of Homeland Security's Cyber Storm II, a multinational cybersecurity exercise that examines security preparedness and response capabilities across a variety of infrastructures.

Mr. Joffe, you are recognized for 5 minutes.

STATEMENT OF RODNEY L. JOFFE

Mr. JOFFE. Good afternoon, Chairman Weiner.

I am, as you say, the senior vice president, senior technologist for NeuStar.

NeuStar provides innovative services that enable trusted communication across networks, applications, enterprises around the world. A major portion of that is involvement with directories. I joined NeuStar in 2006 when UltraDNS, which is a company I founded, was acquired by NeuStar.

DNS is the core directory that really routes traffic on the Internet. Every one of us uses it all the time. Any computing machine makes use of DNS. The technology itself basically deals with the fact that, as humans, we recognize and we are able to use words. Computers understand numbers, in this particular case, IP addresses, and they require the IP addresses to be able to move traffic or to be able to get you from one site to another. The DNS, simply put, is the directory that converts names to numbers and vice versa.

So, for example, if I want to go to www.house.gov, I put that into an Internet browser, and the DNS would convert that to the IP address, 204.141.87.18, and the computing device is then able to get you to the House server, and the screen appears on your computer.

So NeuStar also provides the core directory service for the .biz and the .us top level domains, as well as 17 other top level domains, including a number of other country codes. So, for example, we provide the service for Canada, .ca; for the United Kingdom; and for Japan. We also provide the directory service for anyone attempting to reach many of the Fortune 500 or the e2000 sites. So, in all, we serve about 4,000 corporations and government departments around the world and about 15 million domain names.

I really appreciate you inviting me to speak about the particular threats, and I appreciate the fact that the committee has actually taken an interest.

Probably the oldest reason for Internet attacks is that of ego bragging. There are three real reasons. The perpetrators behind those kinds of attacks are generally young and immature, and they are intent on showing their prowess with computer programming with little or no regard for the damage that they cause in their attacks.

The second and most common category is for financial gain. In this case, the attacks are committed by individuals as well as by organized gangs of criminals. They include large spam e-mail that you have mentioned; the interception and illegal use of computer data, which you have also mentioned, most commonly bank data and credit card data, extortion schemes, which have been around

for quite a while; and Distributed Denial of Service attacks. In DDOS or Distributed Denial of Service Attacks, botnets, which are large groups of thousands, hundreds of thousands, sometimes millions of machines all working together, that have been previously infected, will be used and rented by criminals in the underground. Not only for themselves, but they rent them out. It is a business. The criminal then commands the botnet to try and reach a specific site. The result is that a Web site, for example, is hit by millions of hackers at the same time in an attempt to overwhelm the site and take it down. Frequently, it is successful.

An important thing to note here is that it would require fewer than 10,000 strategically located compromised machines with some reasonable knowledge to disable a sizable portion of the U.S. Internet. It doesn't take many machines.

Generally though the botnets involve hundreds of thousands because the people who build these botnets have no real cost. They are using our resources, and botnets are built almost automatically. We have seen notes where kids go off to school, come back, and take a look at how many bots they have added to their botnet while they have been at school. We have actually seen discussion in the underground about that.

Another lesson on the very dangerous kind of malicious behavior that exists in cyberspace which is known as DNS cache poisoning. This is something that Dan has discovered as you know, last year. Thanks to Dan, we are a lot safer than we were.

But effectively what happens with DNS cash poisoning is that your ISP's caching service are poisoned. The DNS is pointed to a fake site. When you go to your bank, you end up at a Web site that looks just like your bank, but actually isn't. It belongs to criminals. And what they do is they ask you for your password, ask for your user ID, and then they go ahead and make use of that to make transfers and to empty your account.

The third category we talk about is cyberterrorism, which really relates to generally nation-state issues. Over the last 2 years, there have been at least three public attacks reportedly on nation-states. We know that one of them probably is, countries we all recognize Estonia, Georgia and Kyrgyzstan. Additionally, The Wall Street Journal reported on April 8th of this year, as you mentioned, critical infrastructure facilities had been compromised.

It is really important to note over here that, while most people are unaware of the attacks, these attacks are going on all the time, and our industry is reasonably successful in being able to actually stop some of those attacks before they become public. But the attacks are occurring all of the time.

On April 12th, talking about banking, most of this is theoretical, on April 12th, the DNS servers of a major Brazilian ISP, Virtua were compromised. Their cache was poisoned for the entry of one of the largest banks in Brazil, Bradesco, making use of the kinds of things that Dan had talked about. Users of that bank were redirected to a fake Web site, and it took about 5 hours before the bank and the ISP were able to realize that, in fact, the recent entry had been poisoned. The bank was reasonably open in their statement when they said, approximately 1 percent of our customers were affected by this. But that represents almost 150,000 individuals who

could possibly have had their accounts compromised during one event. And this is an event in one country over the course of 5 hours.

The other event is one that you have touched on already, and with indulgence, I will perhaps expand a bit more, which is on the Conficker botnet, the Conficker worm.

We have an industry group called the Conficker Working Group, an unofficial group that came together in the private sector to deal with a real threat, an immediate threat of Conficker. They have been working around the clock to dismantle the botnet with no real success. On the 8th of April, as you said, it took the first steps with version E. You had mentioned earlier that it had upgraded from version D to version E. It wasn't just an upgrade. It was also the first time we got some insight into how the botnet was actually going to be used. It was used to sell fake antivirus. If you have seen those pop-ups on your computer screen, where it may say that you are infected, you normally expect that to show from your antivirus software. In fact, if you were infected with Conficker, there were no messages from your antivirus software. It was actually from the criminal group behind it. They then advertise some software that you could purchase online there and then, enter your credit card, your personal information and download their software. Of course, their software doesn't disable the virus. It installs more malicious software, and the job is now even more difficult.

As a sobering side note on this, last month, in collaboration with one of the other members of the Conficker Working Group from Georgia Tech, we identified at least 300 critical medical devices from a single manufacturer. We stumbled on it. It is not that easy to tell what it is. There were at least 300 medical devices that were infected with Conficker. The hospitals had no idea. The manufacturer had no idea. When we called them, they were obviously shocked. These devices are used in hospitals to allow doctors to view high-intensity scans, MRI for example, CT scans. And they are often found in ICU facilities. They are connected to local area networks. They should never, ever have been connected to the Internet, and according to the manufacturers, they weren't. However, they were connected at some stage to the Internet because they were infected, and they were checking in with us.

The way we know they are infected is that we run systems that those devices will connect to. Worse, after we had notified the manufacturer and the hospitals involved, and we are obviously doing our best for hospitals around the world, we were told that, because of FDA rules that they referred to as 510(k) regulations, 90 days notice was required before the systems could be modified to remove the infections and the vulnerabilities. In some cases, clearly, there can be a disconnect between government rules which are meant to protect consumers and today's cyber threats which sometimes result in delaying and hindering the ability to fix problems as in the medical system.

So based on my long experience in operating large networks connected to the Internet, I think one of the most important areas for Congress to concentrate on is improving the communication both between the public and the private sectors and across those sectors. The Department of Homeland Security operates USCERT, which is

part of its mission to act as a liaison between public and private sectors. It is a start, in my view, but it is woefully understaffed, and it is woefully underfunded for the enormous task that is put before it. Ideally, I would like to see much more focussed collaboration, as that Dan had mentioned and I assume that you have heard before.

In summary, we face enormous escalating threats from all parts of cyberspace both to the economy and to the safety and well-being of many citizens. So, beyond the normal perennial call for additional resources, we need to concentrate on improving the collaboration between industry and government; between different government departments; and between the U.S. and foreign governments.

Mr. Chairman, thank you for the opportunity to address you and the rest of the committee, and I am happy to answer any questions.

[The prepared statement of Mr. Joffe follows:]

16

TESTIMONY OF RODNEY JOFFE
SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST
NEUSTAR, INC.

on

Network Threats and Policy Challenges

before the

Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet
UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

May 1, 2009

TESTIMONY OF RODNEY JOFFE

SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST, NEUSTAR, INC.

Good afternoon, Representative Weiner and members of the subcommittee. My name is Rodney Joffe, and I am the Senior Vice President and Senior Technologist for NeuStar, Inc. NeuStar is a neutral provider of clearinghouse services to the telecommunications industry.

I joined NeuStar in 2006 when we acquired UltraDNS, a company I founded and chaired, and which is the largest provider of DNS services in the world. DNS stands for the domain name system. When a user types in a webname, such as CSPAN.com, DNS is the mechanism that converts the webname CSPAN.com into an IP address, or the numbers that computer networks actually understand, and which are then used to route requests to go to the CSPAN.com web page for example.

Prior to founding UltraDNS, I was Vice President and Chief Technology Officer for GTE Internetworking Business Services, a position I filled as result of GTE's acquisition of Genuity, another of the companies that I founded. At the time of the acquisition, Genuity was one of the largest Internet Service Providers in the world. I also sit on the board of a small number of other technology companies primarily focused in the area of Internet cyber security threats and serve as a member of the ICANN Security and Stability Advisory Committee.

In 2008, I participated in Cyberstorm II, a cybersecurity exercise run by the Department of Homeland Security with participation by four other nations and about 40 private companies from many different sectors. My role was to develop and run the DNS portion of the exercise. While I am not free to discuss the exercise in detail, I can tell you that it was very illuminating to many companies to see just how dependent their operations were on the successful resolution of their DNS and the proper workings of the Internet for the core of their operations.

I am also one of the founders of an unofficial organization known publicly as the Conficker Working Group, established in response to the outbreak and spread of the Conficker Internet worm which first surfaced last year but became much more powerful and threatening in early March of this year. At that time, I briefed a number of Congressional Members, their committee staffs, military and federal law enforcement executives, and industry leaders on the specific threats from Conficker. Conficker represents the state-of-the-art in terms of large scale, malicious Internet and computer malware. Currently, almost 4 million computers around the world are infected with one of its versions. Our experience in coping with Conficker also provides some examples of the holes and gaps in our readiness to defend against and respond to cyber crime and cyber terrorism. I appreciate the opportunity to appear before you today and to bring these examples and facts to your attention.

Everyone understands that cyberspace has no geographic or political borders. Cyberspace is a single place that has not yet been able to properly develop the

natural borders that exist in the real world, borders that you would find for example between states and countries. We don't yet have an effective mechanism to police any of those. So when cybercriminals operate, they have the advantage of being able to use this lack of maturity and are able to ignore the laws and rules that exist in the real world.

In a nutshell, we're still developing the systems and mechanisms that will allow us to conduct ourselves appropriately no matter who we are on the Internet. We are still finding our way. It was only a short while ago that the Internet first came into existence. The security systems that were put in place at the time were never meant for, and could not possibly have envisioned, today's world where nearly every critical piece of infrastructure is tied to the global Internet. And so I really appreciate the opportunity to provide input to the committee, as you look for ways to enhance the security and stability of the Internet from the very real cyber challenges and threats we face today.

The motives for Internet attacks can generally be broken down into one of three categories. The first and oldest reason for Internet attacks is that of ego or bragging rights. In general, and historically, the perpetrators behind these attacks are young, immature and intent on showing their prowess for computer programming, with little or no regard for the damage that they cause in their attacks. Their attacks include website defacements, DDOS attacks and disabling of computers or deletion of files. Probably the most public case was that of the hijacking of Comcast's domain name and website in May of 2008.¹

The second category, now the most common, is for financial gain. Inevitably the hobbyist "miscreants" discover that they can make money doing what they do. In this category, the attacks are committed by individuals as well as organized crime gangs and are manifested in large spam email campaigns, extortion schemes, and the interception and illegal use of computer data - most commonly bank and credit card information. The most public examples of these have been the Russian Business Network², and the McColo Corporation³, one of the most prolific spam outfits. It is important to note in these cases that while some of the facilities were in the US, the principals in these criminal cases operated from Eastern Europe.

The third category and arguably the most worrying, is cyberterrorism, or activities sponsored by nation-states. This category can be further split into two sub-groups: actors who seek to steal national assets and those who would seek the complete destruction or disruption of a country. Over the last two years, there have been at least three public attacks, reportedly nation-state sponsored,

¹ Mills, Elinor "Teens Await After Comcast Attacks." 30 May, 2008. CNET News.
http://news.cnet.com/8301-10784_3-9956165-7.html

² Krebs, Brian "Russian Business Network: Down but Not Out." 7 Nov., 2007.

The Washington Post.
http://voices.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

³ Krebs, Brian "A Closer Look at McColo." 13 Nov., 2008.

The Washington Post.
http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html

against countries including Estonia, Georgia, and Kyrgyzstan⁴, although we now believe that the Estonian and Georgian attacks were carried out for financial rather than political motives. Additionally, there may have been attacks against SCADA (Supervisory Control and Data Acquisition) systems⁵. In New Orleans in January 2008, Tom Donahue from the CIA released information regarding some of these attacks in other countries. There have also been a number of reports of power-generators similar to those used in large US cities being destroyed physically as a result of a cyberattack. The Wall Street Journal reported on April 8 of this year that a federal audit of critical infrastructure facilities in the power industry had been compromised with software that would allow the attackers to disable key elements of the national power grid at will. The sources, identified as "current and former national-security officials" claimed the software was inserted by "cyberspies" from "China, Russia and other countries"⁶.

It is important to understand that the lines between the three categories have become blurred. The juvenile defacers slip just as easily into the role of cybercriminal and cyberterrorist, as do the cyberterrorists slip into the role of cybercriminal.

I'd like to provide some detail around a sampling of real-world events that I've personally been involved in as a way of providing context for some of the challenges and opportunities.

NeuStar operates the core directory that enables data to be correctly routed on the Internet for about 15 million domain names. The technology that enables this capability is DNS, or domain name system. Humans recognize and are able to work with common words and names, however computers only understand numbers and in the case of the Internet, IP addresses, or Internet Protocol addresses. So the DNS, simply put, is the directory that converts names to IP addresses and vice versa. For example, a user enters www.house.gov into an Internet browser and the DNS converts that to the IP address 204.141.87.18. The computing devices are then able to route the user's request to the House's web server.

NeuStar provides this core directory service for the .biz top-level-domain, as well as for 18 other top level domains, including a number of country-code or cc-TLDS. These include .us for the United States, .ca for Canada, .uk for the United Kingdom, .au for Australia, .jp for Japan, and .nz for New Zealand, amongst others. We also provide the directory service for anyone attempting to reach many of the Fortune 500 or eCommerce 2000 companies. All in all, we serve about 4,000 corporations and government departments around the world, and more than 15 million domain names.

⁴ Goodin, Dan "DDoS Attack Boots Kyrgyzstan From Net." 28 Jan., 2009.

The Register. http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/

⁵ Greenberg, Andy. "Hackers Cut Cities' Power." 18 Jan. 2008.

Forbes. http://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html

⁶ Gorman, Siobhan "Electricity Grid in US Penetrated by Spies." 8 April, 2009.

The Wall Street Journal. <http://online.wsj.com/article/SB123914805204099085.html>

The most common kind of attack is called a DOS attack, or Denial of Service attack, whereby an attacker attempts to disrupt the ability of an organization to operate normally on the Internet. In most cases, this kind of attack employs the use of multiple (often tens or hundreds of thousand of machines, and sometimes millions) in a coordinated manner, and in these cases, the attack is classified as a Distributed Denial of Service, or DDOS attack. The attacker takes command of these machines, known as a botnet, and orders the machines to try to reach a specific site. The result is that a website is hit by millions of packets per second in an attempt to overwhelm the site and take it down. While it would require fewer than 10,000 strategically located compromised machines to effectively disable a sizeable portion of the US Internet, these attacks generally involve hundreds of thousands of machines because botnets are easily built. Cybercriminals see them as disposable resources which are easily replaced and at no real cost to the criminals.

In the second kind of attack, the cybercriminals attempt to destroy the computer systems of the victims by overriding data, deleting files, or permanently modifying information.

A third kind of attack revolves around data exfiltration, where cybercriminals attempt to gain access to computer systems either manually or through automated means using viruses, worms or trojans. They then use that malicious software to extract data from their unknowing victim's systems and transfer that data back to the criminals for their own use or blackmarket sale to others. Bank account or credit card information is a frequent target.

There are also a number of lesser-known yet still dangerous kinds of malicious behavior that exist in cyberspace: defacement of websites, where content is replaced, and redirection, where users believe they are directed to one website but are redirected to another website instead. One of the ways this is achieved is through something called DNS cache poisoning, where local copies of the directory are modified by cybercriminals to deceive users. An example of this would be where the customers of a bank are re-directed to a fake bank website that looks identical to their normal banking website, and where the customers then unknowingly provide the criminals with their personal information and banking credentials.

These are but some of the successful threats that we have to cope with today in the Internet security world.

It is important to note that while most people may not be aware of any of these kinds of attacks actually occurring, they are very real. Often, the security industry, through hard work, coordination, knowledge and frequently, pure luck, are able to mitigate the effects before end users notice them. In most cases, these attacks never come to public notice. However, just a few minutes of effort with Google, searching for the terms "DNS and DDoS", and "cache poisoning", and "keystroke logging" will bring thousands of links to reports of successful breaches of Internet defenses. I'll focus on some events that have occurred or have been identified publicly in the last month.

In the first attack, on April 1st, 2009, Register.com, one of the major Internet domain name registrars, was attacked by the use of a DNS DDoS. In this attack,

the attackers caused tens of thousands of compromised computers to flood the DNS or directory servers of the victim with bogus DNS requests, effectively rendering the directory servers unusable. In this particular case, hundreds of thousands of organizations became unreachable because Register.com provided the DNS service for their domains. This attack lasted a number of hours, but the effects lingered for a few days.

A second event occurred on April 12th that is far more insidious for average Internet users. The DNS servers of a large Brazilian ISP, Virtua, were compromised and their cache, or their local temporarily stored domain name and address directory, was "poisoned". The entry for one of Brazil's major banks, Bradesco, was modified by re-directing users to a fake website that was an exact copy of the Bradesco site, but was controlled by cybercriminals. This poisoned entry remained in place for five hours before Virtua and Bradesco noticed the problem and corrected it. According to an official statement from Bradesco, approximately "only 1% of their customers" were affected and potentially re-directed to this malicious site. Unfortunately, 1% of their customers are almost 150,000 individuals and this represents potentially huge monetary losses. Similar cache poisoning events have been occurring for years, and the only complete defense is the implementation of the DNSSEC protocol. However, absent significant effort and support, this solution is unlikely to be available to the general public until 2011 at the earliest.

The third event and perhaps the most visible, in my opinion, is one of the most dangerous botnets ever created. It is based on the Conficker worm which as of today has almost 4 million participating computers. The owners of these computers are unaware that their computers are no longer under their control and a significant number of these computers have been identified as being located inside critical infrastructure networks.

The Conficker worm has the ability of executing many different types of attacks. Modern malware is nothing if not multi-talented; the machines could be used for keystroke logging and data exfiltration or used as a giant online search engine. The botnet could be instructed to search computers local hard drives, as well as all of the systems they are connected to, for any documents or drawings that contain the word "electrical", "secret" or "bank account". They could also be instructed as a group to launch a denial of service attack against any website such as whitehouse.gov or the largest bank in the United States.

As a sobering side-note, over the last three weeks, in collaboration with a researcher from Georgia Tech in Atlanta who is involved with the Conficker Working group, I have identified at least 300 critical medical devices from a single manufacturer that have been infected with Conficker. These devices are used in large hospitals, and allow doctors to view and manipulate high-intensity scans (MRI, CT Scans etc), and are often found in or near ICU facilities, connected to local area networks that include other critical medical devices.

Worse, after we notified the manufacturer and identified and contacted the hospitals involved, both in the US and abroad, we were told that because of regulatory requirements, 90 days notice was required before these systems could be modified to remove the infections and vulnerabilities. We have since identified thousands of infected computers and devices in almost all parts of

critical infrastructure that are infected with Conficker. We are working with industry groups and ISACs to remediate these machines. However it is clear that in some cases, there is a disconnect between government rules meant to protect consumers, and today's cyber threats which sometimes results in delaying and hindering the ability to fix problems, such as in the case with the medical devices.

The news is not all grim, however. There are potential solutions, or at the very least, pathways to defending against these attacks. NeuStar, for example, has developed an interim technology (which can be put in place immediately well before DNSSEC is fully deployed), known as Cache Defender, to provide protection against cache poisoning of the 15 million domains that we are responsible for. Other providers are working on similar innovative solutions.

Based on my long experience in operating large networks connected to the Internet, I believe that one of the most important areas for Congress to concentrate on is in improving the collaboration and communication between the public and the private sectors in dealing with these attacks. The Department of Homeland Security operates US CERT, which as part of its mission acts as a liaison between the public and private sectors. It is a start, but in my view, it is woefully underfunded and understaffed for the enormous task put before it. Ideally, I would like to see a much more focused collaborative effort between the public and private sector--a two way street, where we reach back and forth to help one another. While a lot of US CERT's focus is properly placed on protecting our national infrastructure and our Federal networks and resources, our economy also depends on a multitude of small companies. I would like to see the private partnership role expanded to include not only the major communications and IT companies, but smaller companies as well.

In summary, we face enormous escalating threats from all parts of cyberspace, both to our economy, and to the safety and well-being of our citizens. Furthermore, beyond the obvious and perennial calls for additional resources and funding, we need to concentrate on improving the collaboration between industry and government, and across government departments. It is an enormous task, but one well worth the effort.

Chairman Weiner and members of the committee, thank you for giving me the opportunity to testify on such an important subject.

Mr. WEINER. Thank you, Mr. Joffe.

Our next witness is Larry Clinton. He is the president and CEO of the Internet Security Alliance, an organization that represents corporate security interest and provides a forum for information sharing on information-security issues. Mr. Clinton is also a member of the GAO's expert panel which will make recommendations to the Obama administration on cybersecurity.

Mr. Clinton, welcome. You are recognized for 5 minutes.

STATEMENT OF LARRY CLINTON

Mr. CLINTON. Thank you, Mr. Chairman, and thank you for inviting us to have this hearing, and we are delighted to participate.

Mr. Chairman, virtually our entire economy, our defense system, our culture, now depend on electronic communication systems that are extremely vulnerable and under constant attack. The vast majority of these systems are owned and operated by the private sector.

Unfortunately, virtually all the economic incentives regarding cybersecurity favor the attackers. Attacks are relatively cheap. The area to defend is virtually limitless. Defense residing in separate although connected systems is difficult to coordinate and expensive compared to the return on investment.

The good news is that we know a great deal about how to prevent and stop these attacks. The bad news is, we are just not doing it. The PricewaterhouseCoopers Global Information Security Study of over 1,000 companies found that those that followed the industry best practices could prevent, almost entirely mitigate the attacks against them. The 2008 Data Breach Investigations Report previously referred to studied more than 500 forensic engagements over a 4-year period and concluded that 87 percent of the breaches could have been avoided if reasonable and identifiable security practices had been followed. Robert Bigman, chief of information assurance for the CIA, has stated publicly that most of the attacks that he sees are not that sophisticated, and 80 to 90 percent of them could be prevented with due diligence.

However, we cannot solve cybersecurity problems by attempting to adapt 19th Century models to a 21st Century problem. A common theme from some policymakers who are relatively new to the cybersecurity problem tend to say, well if industry won't do this on their own, we will just have to regulate them. The Internet Security Alliance believes that such an approach is short-sighted and does not reflect the necessary understanding of the new breed of technologies created by the Internet to begin with. Federal regulatory mandates are best designed to combat corporate malfeasance, and that is not the problem we are facing with Internet security.

Even if Congress would enact an enlightened statute, it would only have reach to our national borders, and this is an international problem. A set of U.S. regulations would place U.S. industry at a competitive disadvantage in the global marketplace at the time when we can least afford it.

Specific regulations would likely be too static to the technology, and the threat vectors constantly change; while flexible or conceptual regulations may be too general to have any real effect. Regula-

tions are often subject to political pressure, making minimum standards de facto ceilings, something like what we have with campaign finance.

We need a better system, a 21st Century system. Fortunately, there are signs that the Obama administration understands the need for a modern approach to cybersecurity that appreciates the economic issues as much as the technical ones. President Obama assigned Melissa Hathaway of the National Security Council to conduct a review of our Nation's cybersecurity status. Although the report has not been made fully public, Ms. Hathaway did provide a preview a week ago in Silicon Valley.

Among the specifics from the report she did share was acceptance of the principle that, quote, previous attempts to deal with cybersecurity in isolation have failed in no small part because cybersecurity only succeeds in the context of broader economic progress. In particular, Ms. Hathaway specifically cited the need for government to work with the private sector to, quote, improve market incentives. This is a significant departure from the previous administration's view, which was that the market would emerge spontaneously to address these problems. That did not happen.

Ms. Hathaway is correct. We need to improve market incentives. Consistent with this view, the Internet Security Alliance asks Congress to consider enacting what we call the Cyber Safety Act. The Cyber Safety Act is an affirmative and contemporary approach to dealing with the 21st Century problems of cybersecurity. In brief, we suggest that government's role is not to prescribe mandatory regulation but rather provide market incentives for the private sector entities to adopt the security practices and standards and technologies that have already been empirically demonstrated to work. There are a wide range of incentives which have already been used in various sectors of the economy, such as insurance, liability protections, procurement awards programs, SBA loans, et cetera. All these achieve government goals. What we are suggesting is that these should now be applied to cybersecurity.

Government ought to designate a range of public and private sector entities which can serve as a qualifying set for standards and practices. Government ought to then fund research used to evaluate the standards, practices and technologies developed on an ongoing basis with the sole criteria being their effectiveness. Private sector entities that can demonstrate compliance with the standards and practices would be deemed effective and would qualify for the incentives. What we are attempting to do here through the Cyber Safety Act is to change the economics of cybersecurity by constructing a market that makes private organizations want to continually invest in cybersecurity in their own economic self-interest. Only then can we create the sort of sustainable and evolving system of cybersecurity that we need.

The purpose of this system is to defend the national security's interest, and thus it is worth the relatively modest investment that the government would have to make in order to provide the incentives. The present research and the expert testimony show that by motivating the widespread adoption of the practices that have already been demonstrated to work, the vast majority of the problem we are experiencing can be quickly addressed.

However, there is a small but critical 10 to 15 percent of attacks that will not be addressed in this fashion. My written statement goes into some detail on a number of these problems, including the supply chain, the incongruity with laws that were written in the 1980s to current technology, the need to change the basis for security from protecting the instruments like the computers to protecting the data itself. All of these will require a lot more work than what we are proposing with the Cyber Safety Act.

We look forward to working with the committee both to address the 90 percent of the problem that is basically low-hanging fruit as well as the 10 percent of the problem that is going to require substantially more work.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Clinton follows:]

DRAFT TESTIMONY
LARRY CLINTON, PRESIDENT INTERNET SECURITY ALLIANCE
HOUSE SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
MAY 1, 2009

Mr. My name is Larry Clinton. I am President of the Internet Security Alliance (ISA). The ISA is a cross-sectoral, international trade association operating in collaboration with Carnegie Mellon University. Our mission is to integrate information security technology, business practices and public policy to create a sustainable system of cyber security. It is a privilege to be here.

The Problem

At her confirmation hearings two months ago, Secretary of State Hillary Clinton said that the single biggest threat to our country was the proliferation of weapons of mass destruction, and she identified four categories of these weapons: nuclear, biological, chemical and cyber.

The former Director of National Intelligence Advisor to President Bush, Mike McConnell, has argued that “the ability to threaten the US money supply through a cyber attack is [the] equivalent of today’s nuclear weapon.”

Just 10 days ago, Melissa E. Hathaway, Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, previewed the report on cyber security she has provided to President Obama by saying: “The Internet is neither secure enough nor resilient enough for what we use it for today and will need into the future. This poses one of the most serious economic and national security challenges of the 21st century.”

The cyber security threat is much more serious than the well publicized massive losses of personal data. There are now recorded instances of our government and industry’s electronic infrastructure being compromised by criminals, nation states and even potential terrorists. The result of such attacks could be disastrous ranging from the possible shutting down of our electrical grid to having our own military weapons turned against us.

On a purely economic basis, if a single large American bank were successfully attacked, it would have an order of magnitude representing a greater financial impact on the global economy than September 11. But the threat is not just speculative. Today, cyber security injuries are already substantial: some estimates now place the economic loss from known cyber thefts at more than \$300 million per day.

What We Are Talking About

There are a multitude of cyber security issues being simultaneously discussed in government and industry circles, so it may be useful to begin by placing some boundaries around our testimony.

While many of the solutions the Internet Security Alliance (or ISA) is advocating today have broad impact, our comments today relate primarily to what we call the critical infrastructure protection issues (e.g., protecting the infrastructure, corporate networks and corporate data assets against corporate espionage, Cyber terrorism and Cyber warfare) rather than the “consumer issues” (e.g. privacy/spam etc.).

In addition, there is a good deal of discussion about how the federal government ought to be organizing itself to address the cyber threat. While, as citizens we naturally have our own opinions on our government, as a private sector witness before the Committee representing the ISA, my testimony is focused on how the government ought to partner with the private sector to achieve a national security goal of cyber security, and not how the government chooses to deal with its own internal organizational issues. They are critical issues, but we feel it is vital to emphasize the importance that government place on the role of the private sector as a strong partner in achieving national security goals.

The Energy and Commerce Committee’s Role

The President’s economic initiatives are wholly dependent on the cyber infrastructure. Indeed virtually every element of modern life is now dependent on the digital infrastructure and the vast majority of the electronic infrastructure is in the hands of the private sector. As a result of these facts, our nation’s economic and national security relies upon the security of the assets, properties and operations of the private sector. The interdependency is unlike anything our nation, or any nation, have previously faced in building effective protective strategies.

Traditionally, economic decisions have been made without considering cyber security. Similarly, cyber security decisions have been made without considering their economic impacts. We are now at the point where we must realize that economy and cyber security are opposite sides of the same coin. We cannot address one issue without the other.

Unfortunately with respect to cyber security, virtually all the economic incentives favor the attackers.

Attacks are cheap and relatively easy to conduct. Profits are enormous. The defensive perimeter is virtually endless and defensive measures are expensive

If we are going to develop a sustainable and evolving system of cyber security, we will need to address, and alter, the economics of cyber security.

Moreover, the fundamental reason our systems are currently insecure is that, while private sector organizations will usually invest to protect their own electronic and computer networks and systems, they do not invest adequately to achieve progress

against the broader national security objectives which are properly the government's responsibility. Addressing this imbalance must be part of our solutions in altering the economics of cyber security.

Private corporations are supported by public policy to invest in order to maximize shareholder value, but, in today's environment, maximizing shareholder value does not necessarily equate with government's priorities or government's responsibilities.

The National Infrastructure Protection Plan makes this exact point:

"While articulating the value proposition to the government is clear, it is often more difficult to articulate the direct benefits to the private sector...In assessing the value proposition for the private sector there is a clear national security and homeland security interest in ensuring the collective protection of the nations Critical Infrastructure and Key Resources (CI/KR). Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad scale CI/KR through activities such as...creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted sound security practices."

The Energy and Commerce Committee, with its jurisdiction over so many of the critical infrastructures, including telecommunications, Internet energy, health care as well as commerce trade and consumer protections stand at a critical intersection between economy and security. It is the Energy and Commerce Committee, starting with the Telecommunications and Internet Subcommittee, that is positioned to take aggressive action to provide the market incentives needed to generate private investment in cyber security that goes beyond that demanded by individual business needs and extends this investment to advance against, and helps achieve, our broader national security needs.

The Good News Part One

The first piece of good news is that the Obama administration seems to be embracing the concept that we need to alter our approach to cyber security to include an overall appreciation of the economic aspects of the problem. The administration recognizes the need to enhance market incentives for private corporations to address the broader national security issues raised by our current cyber vulnerability.

When the Obama Administration was elected, the ISA Board proposed a bold new direction in cyber security. Our approach was modeled on the Social Contract that was the underpinning of the development of public utilities, such as power companies and telephone networks a century ago. Our proposal for a Social Contract has been previously submitted to the staff of this Subcommittee.

We advocated that government again engage industry at the business plan level and make it in private corporation's best economic interests to enhance their infrastructure creating a secure cyber network in the public interest.

A century ago, infrastructure development was critically needed and was accomplished in this nation by essentially guaranteeing the return on investments the private sector would need to make. Consumer interests were protected with price and service regulation. In the current environment, the government needs industry's help not to build out the infrastructure, but to secure it.

Just as before, the economic facts demonstrate that generally speaking there is simply not a sufficient return on investment for the private corporations to make the extensive cyber security investments needed to address the broader national interests. Therefore we have advocated a new social contract be struck for cyber security that will, for the first time, address our cyber security issues from as much an economic as a technical perspective.

Just over 2 months ago President Obama assigned Melissa Hathaway of the NSC to conduct a 60-day review of our nation's cyber security status. While the report has not been made fully public, Ms. Hathaway did give a preview a week ago in Silicon Valley.

Among the specifics from the report that she did share was acceptance of the principle that "Previous attempts to deal with cyber security in isolation have failed, in no small part, because they were perceived to be in conflict with the broader societal goals of progress and innovation, civil liberties and privacy rights... Cyber security only succeeds in the context of broader economic progress."

In addition, Ms Hathaway specifically cited the need to work with the private sector "to improve market incentives" for better research development and security management.

This is an important distinction from previous policy. Under the National Strategy to Secure Cyber Space approved in 2002, it was assumed that market forces would simply emerge and that corporations would see the efficiencies of cyber security investments and makes such investments substantial enough to protect the entire infrastructure.

ISA differed with that belief in 2002, and we have persistently asserted that the missing link in that strategy is the lack of market incentives and the need for a public private partnership to create and sustain those incentives.

According to the largest industry survey of cyber security, conducted each year by PricewaterhouseCoopers, a substantial minority---perhaps as much as 1/3 of corporations---will adopt industry best practices completely on their own volition because they see it as good business practice.

However, the majority of private sector entities still regard cyber security investment as a cost center and, while they will make investments consistent with their business plans, the investments are not sufficient to address the broader problem.

Among the alarming findings of recent studies are:

- 29% of senior executives did not know how many security events their firms had
- 50% of senior executives don't know how much money was lost from attacks
- Only 59% of respondents attest to even having an overall security policy
- Nearly half don't know the source of information security incidents
- Only half of respondents provide employees with security awareness training
- Only 43% audit or monitor compliance with security policies
- Just over half of companies (55%) use encryption; 1/3 of don't even use firewalls
- Only 22% of companies keep an inventory of all outside party's use of their data

It is now apparent that the approach in the earlier National Strategy has not worked sufficiently. The laissez faire approach of the National Strategy is inadequate. The security of the Internet can not be left to the invisible hand of the market.

There is considerable debate as to why this finding remains fairly constant. Some say it is a lack of appreciation of the problem. Some say it is the inherent distributed nature of cyber threats, where the host of vulnerability may not be the target of the attack and hence there is not a justifiable return on investment from that particular entity's perspective.

While such a debate may be interesting for some, the ISA regards it as of secondary importance to the issue at hand. The cyber threat to the nation is so real and so dramatic that continuing to debate macro level issues we probably can not resolve quickly is not time well spent, especially when there is so much good that can be done so quickly.

Good News Part II

Fortunately we know a good deal about how to protect our cyber systems; we are just not doing it.

Robert Bigman, the CIA's Chief of Information Assurance told attendees at the October 2008 Aerospace Industries Alliance meeting that, contrary to popular belief, most attacks was not all that sophisticated. Bigman said that with the use of "due diligence" between 80 and 90% of attacks could be prevented. "The real problem is implementation."

Independent research also shows that, when companies follow well established practices of security, they can dramatically reduce the effects of attempted cyber incursions

The "Global Information Security Survey" conducted by PricewaterhouseCoopers found that organizations that followed best practices had reduced downtime and financial impact, despite being targeted more often by malicious actors.

An almost identical finding was reported in the "2008 Data Breach Investigations Report" conducted by Verizon. This study of over 500 forensic engagements over a four year period (including tens of thousands of data points) concluded that 87% of known

system breaches could have been avoided if reasonable security controls had been in place.

Why the Traditional Regulatory Model Won't Work

A common theme from some policy makers who are relatively new to the severity of the cyber security problem is to say, "Well if industry won't do this on their own we will just have to regulate them." ISA believes such an approach is short-sighted and does not reflect a necessary understanding of the new breed of technology and issues created by the Internet.

To begin with, the Federal regulatory mandates are best designed to combat corporate malfeasance, but that is not the problem we face with cyber security.

The problem we have is lack of sufficient investment in cyber security. Regulations will add cost and may not improve security. By adding cost to US firms it may even be counterproductive.

Additional reasons why a centralized US regulatory model will not work are:

- Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and hence would not be comprehensive enough.
- A US law could put US industry at a competitive disadvantage in a global marketplace at a time we can least afford it.
- Specific regulations would be too static as technology and threat vectors change.
- An effort for flexible regulations may be too general to have real effect.
- Regulations may be weaker than needed due to constant political pressure.
- Minimum standards can become de facto ceilings (e.g., campaign finance).
- It would be extremely difficult to enact legislation, wasting valuable time.

A Model for Addressing the Immediate Problem Immediately

For analytical purposes in proposing a model for moving ahead, we will divide cyber threats into two categories. First is the ultra-sophisticated attack such as that carried out nation-state to nation-state, perhaps targeted at high value government targets. Addressing these attacks require specialized longer term interventions which are addressed later in this testimony.

The following part of our analysis deals with the second, much larger, category of risks, which comprises the vast majority of attacks both upon government and private enterprise resources and assets. These are the risks associated with known threats and vulnerabilities for which existing best practices can be a strong defense.

The research, as well as expert testimony, informs us that existing technologies and best practices can and will resolve or mitigate large portions of our core cyber security problem, namely our vulnerability to known cyber attack methods and tools. However,

there are multiple different sets of technologies, standards and practices in the marketplace. While the patterns of attacks and threats are constantly changing, there is consistency in the types of resources to deploy as effective defenses. To build an effective and sustainable system of cyber security that advances our national objectives, three items must be considered:

- A. How are we to establish which standards and practices and technologies are to be encouraged?
- B. What do we encourage compliance with the approved standards, practices and technologies?
- C. What is the best way to measure compliance in order to award benefits?

Standards of Care Ought to be Based on What Works

There is a tremendous similarity in the business and security practices the research indicates work against vulnerabilities and risks.

The PricewaterhouseCoopers world wide study of more than 10,000 corporations isolated 7 items which characterized their "best practices group" which almost entirely escaped the effects of attacks on their systems"

- a) Spend on Security ---best practices companies tended to spend nearly 30% more on information security than the average organization.
- b) Separate information security from "IT." Cyber security is not an IT issue, it is an enterprise wide risk management issue and successful firms treat it as such.
- c) Penetration testing quarterly to patch up network and application security.
- d) Conduct security audits to identify threats to employees and corporate IP.
- e) Complete a comprehensive risk assessment to classify, prioritize threats and vulnerabilities.
- f) Define an overall security architecture and plan based on the previous steps.
- g) Conduct quarterly reviews with metrics to measure effectiveness.

The 2008 Verizon study evaluated 500 forensic investigations over a 4-year time period and found in 87% of the cases, compliance with 10 practices that worked could have prevented the attempted breach from being successful. Their lessons were:

- a) Align process with practice. In 59% of breaches organizations had policies in place that may have prevented the breach, but failed to follow them.
- b) Achieve the essential then worry about the excellent. 83% of breaches were achieved by attacks not considered highly difficult to handle, but many organizations were apparently so focused on stopping sophisticated attacks they failed to take care of the basics.

- c) Secure business connections with partners. Nearly 40% of breaches were associated with business partners and might have been prevented with basic business partner facing security practices.
- d) Create a data retention plan. 66% of breaches involved data the victim didn't know was on the system. A comprehensive plan ought to force organizations to understand where their sensitive data is and take appropriate steps to protect it.
- e) Control data with transaction zones. Once data is properly categorized it can be placed in an appropriate zone to allow for more sensitive data to receive more comprehensive security.
- f) Monitor event logs. In 82 % of cases studied, information about events leading up to the attack was available and either went unnoticed or not acted upon.
- g) Create an incident response plan. If and when a breach is suspected an effective response plan can ensure that the breach is stopped before data is fully compromised.
- h) Increase awareness among employees. Increased awareness can increase timely reporting and prevent incidents as well as assist in mitigation and recovery.
- i) Engage in mock testing, on a mandatory and routine basis.

Government's Role

Government's first role (apart from getting its own house in order) ought to be to encourage the broader adoption of the security practices that have already been demonstrated to be effective.

This encouragement should take two forms. First, entities, beyond the early adopters of these effective best practices, should be encouraged to emulate them and adopt these, or appropriately similar, practices. Second, the already-identified effective practices need to be continually adapted to keep pace with the changing technological and security needs that are inherent parts of the cyber-landscape.

Government can provide vast assistance to this effort by fashioning an incentive program for the good actors that will create a business advantage for them over less careful players by rewarding positive behavior (similar to how doctors and hospitals are receiving economic incentives to adopt electronic patient records). In so doing, the power of the market can be harnessed to motivate improved cyber security. Since many of the organizations targeted are in fact international, improvements on a worldwide basis are possible.

Part of such a program ought to be an evaluation component which will provide a real world replication study of these practices and revisions based on these follow up studies. Evaluating and measuring results is a powerful contribution to continually improving security practices.

Government ought to identify multiple entities (both public and private) which would be able to identify standards and practices that would be eligible for market incentives.

It is important that the government not set a single set of standards. Government can be subject to political pressure, and can be challenged to deal with the vast and ever-changing array of needs companies actively contributing to the US economy, many not US-based, may face. In addition there may likely be strong international resistance to standards solely determined by the US government. Perhaps more important, the notion of one size fits all does not recognize the reality of multiple business sizes, cultures, regulatory regimes degree of criticality within the infrastructure and business plans.

Our model contemplates that government encourage security adoption by defining targets of effectiveness to be achieved and providing incentives that are awarded based on achieving those objectives. It would be more appropriate to establish a tiered set of standards and practices that would allow companies to balance the criticality of the information they are protecting with their investment tolerance. We will protect an education system or a social network differently than we will protect our critical energy infrastructure or a military C2 network. Standards would naturally be different for each, so a tiered standard set that would recognize different levels of security and risk management is appropriate.

The various tiers could then be mapped to the qualifying incentives to these various levels of compliance (e.g. level “x” yielding tax incentive “a” and level “y” yielding tax incentive “b”).

Government’s interest is not in assuring compliance with any particular set of technologies, standards or practices, but rather achieving the efficacy of the intervention. Therefore, it makes little difference how the industry meets the effectiveness levels established as qualifying for the incentive, but simply that their investments are judged as effective and deserving of award of the available incentives.

The government’s second role would be to select and fund independent research of the interventions created by the approved agencies. Entities would be able to remain on the list of qualifying standard and practice setters only based on the efficacy of their standards as determined by independent studies.

At the outset we propose companies have available federal incentives if they implement information security pursuant to and meet the:

- Information security procedures adopted by a Federal sector-specific regulatory agency.
- Standards established and maintained by the following recognized standards organizations:
 - International Standards Organization
 - American National Standards Institute
 - National Institute of Standards and Technology
- Standards established and maintained by an accredited security certification organization or a self-regulatory organization such as NASD, BITS, or the PCI structure.

- Private entities such as insurance and audit firms who can demonstrate either a financial interest in quality compliance or independent research.

Creating Incentives for to Promote Good Security Behavior

The application of good standards is a measure of due diligence not ironclad security.

Moreover, for both large and small companies, it is often difficult to find the money to implement desired security practices across the organization when there is no apparent business return on investment. Since securing the infrastructure writ large is the government's responsibility, an incentive system needs to be put in place to assure that private companies will meet this need in the absence of a purely business reason to do so.

The notion of providing market incentives for industry to accomplish pro-social needs as a proxy for the government exists broadly throughout our economy and history with the original social contract being only a paradigm case. We simply have not yet applied these principles to cyber security.

The following is a list of incentives, many of low or virtually no cost to the public, which can be used to alter the economic perspective with respect to investment in cyber security procedures and thus encourage private entities to improve their security posture in the broad national interest.

1. Create a Cyber Safety Act. The SAFETY Act, passed after 911 to spur the development of mostly physical security technology by providing marketing and insurance benefits, could be adapted to provide similar benefits for the design, development and implementation of cyber security technology, standards and practices.

By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, practices and standards, these organizations can similarly use the marketing and insurance benefits, thus providing business benefits to extending their cyber security spending beyond what is initially justified by their business plans. The program has been successful in the physical arena. [any examples??]

2. Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices. Using model described above for selecting standards and practices make on-going eligibility for federal grants and loans contingent on compliance with identified security practices. This is a proven and successful method for advancing broad policy objectives (e.g., non-discrimination in employment).

Among the benefits of this approach is that there is no significant impact on the federal budget since this money is already designated for distribution. There is also the potential for relatively immediate impact since it utilizes current standards, practices and government programs. In addition this approach allows for adaptation to future needs since most applications must be periodically renewed. Finally, a renewal process in place for these types of government contracts allows for compliance testing as a means of approving and continuing the contract... The reach of the positive effect of this approach will go beyond major players to include broader universe of suppliers and contractors to CI/KR.

3. Leverage Purchasing Power of Federal Government. Government could increase the value of security in the contracts it awards to the private sector, thus encouraging broader inclusion of security in what is provided to government.

This approach could facilitate broad improvement of the cyber security posture among CIKR owners and operators by “building in” security from the beginning in products and services that are developed and delivered to the government. If the requirements were extended to suppliers and sub-contractors as well, this initiative could have a significant affect on down-stream entities as well.

While this approach does have substantial potential benefit, government would need to enhance the value of the contracts since not all the organizations in the supply chain have the same massive incentive to adopt government specifications that some large players do. This approach has potential for real and immediate benefit, but it is important that government realize that such compliance cannot be expected to come “for free”. National security has a cost and it is the government’s responsibility to pay it.

4. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks addressing information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, and state regimes could be analyzed to create unified compliance mode for similar items & eliminate any overlaps. Sector specific requirements could be identified, of course, but effective security has many similar elements. Duplicative regulations impose a cost on industry that ultimately increases their resistance to prioritizing compliance.

If compliance with one set of regulations were to be considered as compliance with all, the reduction in compliance costs would allow for the freeing of resources to be returned to security as opposed to compliance efforts.

5. Tax incentives for development of and compliance with cyber security standards practices and use of technology. Using our model described above for selecting standards and practices, the receipt, and on-going eligibility for, tax credits can be made contingent on compliance with identified security practices.

While tax incentives are often difficult politically, this approach may be targeted to smaller and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and may otherwise never perceive compliance with effective cyber security practices to be economically beneficial.

6. Grants/Direct Funding of Cyber Security R&D. The Federal Government could give grants to companies developing and implementing cyber security technologies or practices. Alternatively, R&D could be run through one or more of the FFRDCs. This would reduce the private-sector cost of developing and deploying cyber security technologies.

7. Limit liability for good actors. The Federal Government could create limited liability protections for certified products and processes, such as those approved under the modified SAFETY Act proposal, or those certified against recognized industry best practices. . Alternatively, liability might be assigned on a sliding scale (comparative liability), such as limiting punitive damages but allowing actual damages and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.).

Liability costs are among the most sensitive issues confronting senior corporate executives and a long-standing target for reform. Tying adherence to best practices and standards to a limitation in liability might be extremely effective in building a business case for extended cyber security investment. There is no such thing as perfect security, but one of the biggest concerns within industry is that, despite making the best possible investments in security, a court would still impose liability for a one-in-a-million hostile attack that succeeds. That outcome is not in the best interest of the public policy of improving security.

In making this proposal, our objective is to provide incentives to those who make authentic investments in improved security, consistent with the standards and best practices that are incorporated into an overall Government program. That objective stands in contrast to those who may argue that there should be no liability at all.

8. Create A National Award for Excellence in Cyber Security. The Government could create an award for companies that adopt cyber security best practices (e.g., the Malcolm Baldrige Award by the Department of Commerce).

This is a low cost effort with substantial benefits. Organizations may strive to receive the award as a means of differentiating themselves in marketing; consumers will value companies that have this type of recognition, particularly in a marketplace in which their security concerns continue to increase.

9. Promote Cyber Insurance. Cyber insurance, if more broadly utilized, could provide a set of uniform and constantly improving standards for corporations to

adopt and be measured against, while simultaneously transferring a portion of risk the Federal government might face in the case of a major cyber event. Insurers require some level of security as a precondition of coverage, and companies adopting better security practices 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 cyber-security. 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 responsive to updating as necessary to respond to new risks. Insurers 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 to 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. Insurance companies can also provide a market based monitoring and assessment function thus reducing the cost to the government while assuring compliance with ever increasing standards and practices.

The Government could assist in bringing about these changes by (1) creating a Cyber-Safety Act as I discussed earlier, (2) fund or support necessary R&D efforts by the insurance industry, (3) provide temporary "reinsurer of last resort" support in cases of massive cyber events (so called "cyber-hurricanes"), (4) require cyber-insurance for those contractors that touch governmental data or systems and (5) encourage the purchase of cyber-insurance thorough use of the "government podium".

How Best to Monitor Compliance

It is sometimes blithely asserted that if the private sector doesn't do a better job of cyber security the government will simply have to regulate them.

Often these assertions are followed by suggestions that Sarbanes/Oxley/GLB or HIPPA standards could simply be expanded.

Leaving aside the broad policy problems with these simple solutions which are articulated above, research suggests that such expansion of government regulation is unlikely to succeed even if enacted.

The previously referenced PricewaterhouseCoopers study reported in the October 2008 edition of CIO Magazine that only "44% of respondents say they test their organizations for compliance with whatever laws and industry

regulations apply.” The study notes that this is an increase in compliance, but it is extremely noteworthy that several years after these laws and their regulations (such as HIPAA and Sarbanes-Oxley) have been in effect, less than half of the surveyed companies are even testing for compliance.

CIO magazine goes on to note “many organizations aren’t doing much beyond checking off the items spelled out in regulations--and basic safeguards are being ignored” (which is consistent with the findings of the 2008 Data Breach Investigations Report cited earlier).

The federal government’s lack of success in getting federal agencies to meet their own FISMA requirements also suggests this is not an area the federal government does well. It is impractical for the federal government to take on the massive role of determining, monitoring and constantly adjusting cyber security requirements funded only by tax dollars.

Far more practical would be for the federal government to use its resources to establish a functional private sector system which the federal government could participate in and where necessary regulate. Insurance companies are the best available vehicle for such a program.

The insurance industry is in a uniquely motivated to understand and communicate to its insured’s what are the standards of due care appropriate for the management of network security because they have “skin in the game”. That is to say, in the event of a loss it is the insurance company that will pay excess of any self-insured retention, and any damages to third parties as well as reimburse the policyholder for any loss of business and additional expense associated with the event.

A robust cyber insurance industry, operating under traditional regulatory regimes, could serve the public interest by providing a mechanism for continually upgrading security practices and standards, monitoring compliance and reducing governments risk exposure in the event of a cyber hurricane.

Longer Term Issues and Solutions

While the model outlined above would make substantial progress in addressing the vast majority of current cyber risks, there remain a range of sophisticated issues which will not be adequately addressed by implementing best practices.

As part of the process for Melissa Hathaway’s 60-day review Board members of the Internet Security Alliance provided policy papers addressing some of the more difficult issues for the nation. These papers are provided as appendices, but are summarized below:

A Model for Cyber Protection by Disrupting Attacker Command & Control Channels Jeff Brown Raytheon

There is no way to prevent a determined intruder from breaking into a system that uses e-mail and web surfing and no business can survive without these tools of the information age. Raytheon CISO Jeff Brown proposes that in addition to focusing on preventing attackers from getting into your system we should also focus on detecting and disrupting the attackers command and control communications back out of our networks, thereby leaving them unable to exfiltrate vital data. While some of the process Raytheon uses in effecting this strategy are probably practical only for firms with the size and resources of a Raytheon some of the collaborative processes Raytheon uses are practical for organizations of all sizes. There are substantial incentives for participation at all levels with implications for government industry relations, private sector models of threat and vulnerability detection and information sharing.

Information Security for the Next Century
Dr Pradeep Khosla Dean Carnegie Mellon University Engineering and Computer Science

Operating from many of the same premises as Jeff Brown, Carnegie Mellon University's Dr. Pradeep Khosla also suggests the need for approaching information security through an entirely different model. Dr. Khosla suggests an information centric approach which shifts the focus of protection from the devices (computers/USBs etc.) and instead seeks to secure the data itself with security policies are applied to the data itself with the policies embedded in the data thus making it self-protecting. Dr. Khosla argues that with the rise of virtualization information security will inevitably become information centric.

Securing the Globalized IT Supply Chain a Strategy and Framework
Scott Borg Director US Cyber Consequences Unit

There is a serious danger that the supply chain for electronic components, including microchips, could be infiltrated at some stage by hostile agents. These hostile agents could alter the circuitry of the electronic components or substitute counterfeit components with altered circuitry. The altered circuitry could contain "malicious firmware" that would function in much the same way as malicious software. If the electronic components were connected to any network that enemy attackers could access, the malicious firmware could give them control of the information systems. A logic bomb in a weapons system could shut down the larger information system or, worse, turn the equipment controlled by the information system against those operating it.

Once malicious firmware has been inserted into electronic components, it can be almost impossible to detect. Because it is in the hardware, the malware will remain in place even when all the software has been upgraded or replaced. Building on a series of conferences ISA conducted with Carnegie Mellon US Cyber Consequences Director Scott Borg describes a strategy and framework though which this complicated technical and economic problem can be managed long term.

Adapting 20th Century Regulations to the 21st Century Technologies
Jeffrey Ritter, CEO, Waters Edge Consulting

Governments, corporations and the courts have struggled to interpret the applicability of privacy statutes enacted in the 1980s and 1990s to the rapidly evolving technologies and communication services that have been built upon the platform of the Internet. Many of the critical words used in the 20th century laws have proved difficult to apply to 21st century technologies—key terms such as “intercept”, “record”, “monitor”, “electronic communication”, “contents”, “transmission” were not drafted with a focused capability to adapt to evolving Internet services.

At a time in which US companies are desperately looking to find new operational efficiencies and improve their competitive capability in a global, wired market, the existing legal issues created by these 20th century laws are inhibiting sound, productive investments in UC solutions. Simply stated, companies are genuinely concerned that they are unable to employ modern, conventional Internet security services across UC solutions without exposing themselves to legal sanctions and possible prosecution. WatersEdge CEO Jeffrey Ritter outlines the study he has taken at the request of the ISAlliance Board to develop business models to adapt to this confusion which may yield policy implications as well.

Technology to Enable Effective Information Sharing
Joe Buonomo, President Direct Computer Resources

Even though, Government is uniquely positioned to coordinate intelligence collection and analysis and provide sanitized threat and vulnerability information to the private sector there has been a certain reluctance not to do so because of the classified nature of the information.

Joe Buonomo, of Direct Computer Resources, Inc. (DCR), believes that there is currently industry-proven, off-the-shelf technology that has become widely available in recent years which can ameliorate this reluctance and incline Government to make this information more readily available to the private sector.

Although this technology in itself won't instantly resolve complex issues in government any more than it does for industry, DCR contends that it will provide a means through which any government agency can safely provide selected critical information to another or to industry sectors on a need-to-know basis and without exposing classified data. Allowing the free flow of critical information on a timely and secure basis should provide government agencies and the private sector with enough time necessary to react to a potential threat and nip it in the bud.

Thank you Mr. Chairman I will be happy to answer any questions the Committee may have.

Mr. WEINER. Thank you, Mr. Clinton.

Our final panelist before we begin questions is Gregory Nojeim. He is the senior counsel and director of the Project on Freedom, Security and Technology at the Center for Democracy and Technology. He has been integral in bringing together broad coalitions from across the political spectrum to limit the threats to privacy and civil liberties posed by government monitoring of the Internet and other communications.

Mr. Nojeim, you are recognized for 5 minutes.

STATEMENT OF GREG NOJEIM

Mr. NOJEIM. Thank you, Chairman Weiner.

It is really a pleasure to testify today on behalf of CDT. Our organization is a nonprofit organization, and we are dedicated to keeping the Internet open, innovative and free.

So it won't surprise you that most of my comments today will focus on the communications infrastructure as opposed to other infrastructure systems and, in particular, on the Internet.

Cybersecurity policies should distinguish between government systems and systems that are owned and operated by the private sector. Policy toward government systems can be much more prescriptive. It can be much more top-down than policy toward private systems.

Congress should also distinguish between the elements of the critical infrastructure operated by the private sector that primarily support free speech and those that do not. As an example, measures that might be appropriate for securing the control systems of a pipeline, they might not be right for securing the Internet. It might be wise, for example, to require a particular kind of authentication of a user of an information system that controls a pipeline. But it might not be wise to require that same kind of authentication for a computer user in the privacy of their own home while they are surfing the Internet.

The characteristics that have made the Internet successful, openness, decentralization, user control, things that you mentioned in your opening statement, Mr. Chairman; these things can be put at risk if heavy-handed cybersecurity policies are applied to all critical infrastructure. This subcommittee should make protection of these attributes an essential part of its cybersecurity mission.

It is also important to ensure that cybersecurity measures do not result in a governmental entity monitoring private communications networks for intrusions. Monitoring these systems is the job of private sector communications providers, and they already do this.

The government can help them do a better job. It can help them develop tools that allow communications providers to monitor for intrusions in the least intrusive way. But it should not be in the business of monitoring private networks itself. Nor should the government be in the business of shutting down Internet traffic to compromised critical infrastructure information systems in the private sector.

While some have proposed giving the President this extraordinary power over all critical infrastructures, we believe it should extend only to governmental systems. Such authority applied to private systems would empower a President to coerce unwise, even

illegal activity. To our knowledge, no circumstance has yet arisen that would justify a Presidential Order to cut off Internet traffic to a private critical infrastructure system when the operators of that system think it should not be cut off.

We also urge you to carefully address two overarching recurring cybersecurity policy problems. The first is excessive secrecy. The subcommittee should work to improve the transparency of the cybersecurity program. Transparency builds trust with the private sector, and that is essential to foster its cooperation. It also enhances public understanding of the nature and justification for any impact on users of cybersecurity measures. Transparency also promotes essential accountability.

The second overarching problem is improving information sharing between the private sector and the government. Starting with the right questions about information sharing will help in settling on the right answers.

Exactly what information held by the private sector has not been shared with the government when it was specifically requested? What reasons were given for the decision not to share? Why aren't existing information-sharing structures—I am sorry. Why are existing information-sharing structures like USCERT falling short? And what additional market incentives would encourage the private sector to share threat and information solutions? Generally, as you approach these and other cybersecurity problems, we urge you to favor market-based measures over mandates. And we ask that you consider carefully the impact on the Internet of measures proposed for securing all critical infrastructure systems. Thank you.

[The prepared statement of Mr. Nojeim follows:]

Statement of Gregory T. Nojeim

**Senior Counsel and Director,
Project on Freedom, Security & Technology
Center for Democracy & Technology**

**Before the House Committee on Energy and Commerce,
Subcommittee on Communications, Technology and the Internet**

**On
Cybersecurity, Civil Liberties and Innovation**

May 1, 2009

Chairman Boucher, Ranking Member Stearns and Members of the Subcommittee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.¹ We applaud the Subcommittee's leadership and foresight in examining the challenges we face as a nation in addressing cybersecurity issues in a manner that reflects our commitments to liberty and market-driven innovation.

The Cybersecurity Threat

It is clear that the United States faces significant cybersecurity threats. Recently, the *Wall Street Journal* reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.² U.S. intelligence agencies, which have developed capabilities to launch cyber attacks on adversaries' information systems, have sounded alarms about what a determined adversary could do to critical information systems in the U.S.

It is also clear that the government's response to this threat has been woefully inadequate. The Department of Homeland Security has been repeatedly criticized³

¹ The Center for Democracy & Technology is a non-profit, public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom after September 11, 2001. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications and public interest organizations, companies and associations interested in information privacy and security issues.

² Gorman, Siobhan, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal*, <http://online.wsj.com/article/SB124027491029837401.html>, April 21, 2009. See also, Gorman, Siobhan, Electricity Grid in U.S. Penetrated by Spies, *The Wall Street Journal*, <http://online.wsj.com/article/SB123914805204099085.html>, April 8, 2009.

³ See, e.g., Government Accountability Office, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* <http://www.gao.gov/new.items/d061087t.pdf>, Testimony of GAO's David A. Pownier, Director, Information Technology Management Issues,

for failing to develop plans for securing key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, and information technology and telecommunications systems, as required in the Homeland Security Act of 2002.⁴

In recognition of these risks and challenges, President Obama ordered his national security and homeland security advisors to examine the cybersecurity issue and develop for him a policy blueprint. Melissa Hathaway headed the 60-day review. The review team reported to the President on April 17, but its recommendations have not yet been made public. The review team solicited input from a wide range of cybersecurity stakeholders, including the privacy and open government communities.⁵ The Administration should be commended for its process.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. It is absolutely essential to draw appropriate distinctions between government systems and systems owned and operated by the private sector. Policy towards government systems can, of course, be much more “top down” and much more prescriptive than policy towards private systems.

With respect to private systems, it is further necessary when developing policy responses to draw appropriate distinctions between the elements of “critical infrastructure” that primarily support free speech and those that do not. The characteristics that have made the Internet such a success – its openness, decentralized and user controlled nature and its support for innovation and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all “critical infrastructure.”

Almost 20 years ago, the Commerce Committee played a key role in opening the Internet to commercial traffic. Since then, it has largely promoted a light-handed

before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, September 13, 2006. Last year, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team (“U.S. CERT”), which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a “truly national capability” to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, <http://www.gao.gov/products/GAO-08-588>, July 2008.

⁴ P.L. 107-296, Section 201(d)(5).

⁵ CDT hosted a meeting among privacy and open government advocates, and Ms. Hathaway and her key staff on March 4. CDT submitted recommendations to the 60-day review team; those recommendations can be found in this March 19 letter to Ms. Hathaway: http://www.cdt.org/security/20090319_cybersecure_comments.pdf.

approach to governmental regulation of the Internet that has helped it become a ubiquitous and valuable part of the American economy and democracy. We ask this Subcommittee in particular to enter the cybersecurity policy debate with this history in mind, and with the mission of protecting the attributes of the Internet that make it so important to free speech. The Internet is different from other critical infrastructures; it is time to say so.

While the Internet is a “network of networks” encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the network into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers. Approaches to cybersecurity that would eliminate pseudonymous and anonymous speech online would put privacy at risk, chill free expression and erode the Internet’s essential openness. As the founders of our country recognized, anonymity and pseudonymity play essential roles in allowing political views to be aired.

In sum, CDT believes that cybersecurity legislation should not treat all critical infrastructure information systems the same. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet and communications structures critical to new economic models, human development, free speech and privacy are not regulated in ways that could stifle innovation or chill free speech.

Communications Network Providers – Not the Government – Should Monitor Their Networks for Intrusions and Respond To Such Intrusions

Most critical infrastructure computer networks are maintained by the private sector. Private sector operators already monitor those systems on a routine basis to detect and respond promptly to any possible attacks, and it is often in their best business interest to continue to ramp up these defenses.

CDT strongly believes that no governmental entity should be involved in monitoring private networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. Instead, the government should help develop the tools that allow providers to do this in the least intrusive way. Effective cybersecurity does not require that backbone providers give governmental entities access to the communications that flow through their networks.

The government has a legitimate role, to the extent it has any special expertise, in helping the private sector develop effective monitoring systems to be operated by the private sector. The government also should be sharing information with private sector network operators that will help them identify attacks at an early stage,

defend in real time against attacks, and secure their networks against future attack. Most of the federal government's cybersecurity effort should focus on these forms of interaction with the private sector.

When an attack occurs, or when events suggesting a possible attack are observed, private sector providers may need to share with the government limited information that is necessary to understand possible attacks, respond, and resist further attack. The Wiretap Act and the Electronic Communications Privacy Act already contain self-defense provisions that are broad enough to permit the sharing of communications information from the private sector to the government that is necessary to respond to an attack. See 18 U.S.C. 2511(2)(a)(i), 18 U.S.C. 2511(i), 18 U.S.C. 2702(b)(5) and 18 U.S.C. 2702(c)(3). In CDT's view, no new statutory authority is needed to broaden this flow of information; rather, Congress should require public statistical reporting on the use of these provisions. Moreover, these provisions should be narrowly construed in the cybersecurity context to apply only when a company believes it is or may be under attack or that an attack has occurred. They cannot justify ongoing or routine disclosure of traffic by the private sector to the government.

Some have proposed that the President ought to be given authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency, or to disconnect such systems from other networks for reasons of national security.⁶ Such extraordinary power should extend only to governmental systems, not to those maintained by private sector entities. Even if such power over private networks was exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. Any such shut down could also have far-reaching, unintended consequences for the economy and for the critical infrastructures themselves. To our knowledge, no circumstance has yet arisen that could justify a Presidential order to limit or cut off Internet traffic to a particular critical infrastructure system when the operators of that system think it should not be limited or cut off. They already have control over their systems and financial incentives to quarantine network elements that need such measures. We urge you to reject proposals to give the President or another governmental entity power to limit or shut down Internet traffic to privately-held critical infrastructure systems.

Transparency in the Cybersecurity Program Promotes Trust and Industry Participation

So far, the government's cybersecurity efforts have been shrouded in too much secrecy. Openness is necessary for ensuring both that the public understands the nature of and justification for any civil liberties impact and that the public can hold the government accountable for the effectiveness of its efforts and for any abuse of its powers. To protect privacy and civil liberties and to encourage private sector

⁶ Section 18 of the Cybersecurity Act of 2009, S. 773.

trust and participation, the government must make public more information about existing threats, the measures being taken to protect the relevant networks, and how those measures could affect individual users.

Not every detail of every aspect of the federal cybersecurity program needs to be revealed. In fact, many details should remain classified so that those attempting to breach sensitive networks are not provided with information that could aid them. For example, information collected by intelligence agencies that describe the attack signatures of foreign adversaries or their capabilities must be handled very carefully. However, the level of secrecy toward cybersecurity in the last Administration put the success of the program at risk by not providing enough information for the public to understand what the government was trying to do, the role of the private sector, and how privacy would be protected.

The lack of transparency also undermines trust and cooperation with the private sector entities that operate much of the critical infrastructure that must be protected against attack. Private sector entities also provide much of the hardware and software used by government systems, including classified systems, and are likely to have valuable information about vulnerabilities, exploits, patches and responses. No policy response to encourage a more robust public-private partnership on cybersecurity will be effective unless and until the government brings its cybersecurity efforts out of the shadows.

Promoting Information Sharing Between the Private Sector and the Government

There is widespread agreement that information sharing is an important component of an effective cybersecurity strategy and that information sharing today is inadequate. However, there is no clear consensus on how to improve information sharing. We do not need information sharing merely for the sake of sharing information. It is important that the information that is shared is the information that is actually needed and is actionable, and that adequate standards and privacy protections be put in place when the information to be shared includes personally identifiable information.

Improving information sharing should start with a discussion about exactly what information held by the private sector has not been shared with the government when a specific request for it has been made, and the reasons given for the decision not to share the information. Next, there needs to be an understanding of why existing structures are falling short. These existing structures include the DHS U.S. Computer Emergency Readiness Team ("U.S. CERT"), which already has an information sharing role, and the existing public private partnerships represented by the Information and Analysis Centers ("ISACs").⁷ These structures should be

⁷ Each critical infrastructure industry defined in Presidential Decision Directive 63 (1998) has established an Information Sharing and Analysis Center to facilitate communication

fixed or eliminated before consideration is given to creating new information sharing structures. The GAO recently made a series of suggestions for improving the performance of U.S. CERT.⁸ They included: giving it analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority.

Regardless of the structure used, it seems that industry self-interest, rather than government mandate, should be enhanced to facilitate information sharing. Congress should explore whether additional market incentives could be adopted to encourage the private sector to share threat and incident information and solutions. One option would be to compensate companies that share with a clearinghouse the cybersecurity solutions in which they had to invest substantial resources. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. Congress should consider whether an antitrust exemption to facilitate cybersecurity collaboration is also necessary. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information.

CDT strongly disagrees with proposals to solve the information sharing dilemma by simply expanding government power to seize privately held data. We urge the Subcommittee to steer clear of a recent proposal to give the Secretary of Commerce unfettered authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities, regardless of whether the information to be accessed is proprietary, privileged or personal and without regard for any law, regulation or policy that governs governmental access, including privacy laws like the Electronic Communications Privacy Act.⁹ This approach is dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. We urge you to reject this heavy-handed approach, and to instead favor market-based incentives to facilitate information sharing.

DHS Should Lead, with Augmented Resources and High Level Support

It is widely expected that the President will decide it is necessary to provide greater

among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. The ISACs are linked through an ISAC Council, <http://www.isaccouncil.org/> and they can play an important role in critical infrastructure protection, as indicated in this white paper from January, 2009. http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf

⁸ Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, <http://www.gao.gov/products/GAO-08-588>, July 2008.

⁹ Section 14 of the Cybersecurity Act of 2009, S. 773.

cybersecurity leadership from the White House and that seems generally appropriate. Some have suggested that the DHS National Cyber Security Center (NCSC), which now leads the government-wide cybersecurity program, should be moved to the National Security Agency, which would then oversee the program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government. However, expertise in spying does not necessarily entail superior expertise in cybersecurity. Moreover, there is serious concern that if the NSA were to take the lead role in the cybersecurity initiative, it would almost certainly mean less transparency, less trust, and less corporate and public participation, increasing the likelihood of failure or of ineffectiveness. Citing many of these concerns, as well as a lack of adequate resources, the Director of the NCSC recently resigned in a stinging, public letter.¹⁰

In part, distrust in the NSA emanates from its recent involvement in secret eavesdropping activities that failed to comply with statutory safeguards. The program placed private sector companies asked to assist with the surveillance in an extremely difficult position; those that provided assistance were exposed to massive potential liability.

The concerns with NSA go beyond the recent activity. NSA has long had a dual role: it spies on adversaries, cracks their computer networks, and breaks their codes. It also protects U.S. government communications from interception. These two roles tug in opposite directions because the U.S. and its adversaries frequently use the same technology.¹¹ As a result, if NSA finds a security vulnerability in a widely used product, it may be inclined to keep the loophole a secret so it can exploit the vulnerability against its targets. This would deprive other government agencies and private entities of information they could use to defend themselves against attack.

Finally, NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. NSA should not be given a leading role in monitoring the traffic on civilian government systems, nor in making decisions about cybersecurity as it affects such systems; and its role in monitoring private sector systems should be even less. Indeed, NSA Director Lt. Gen. Keith Alexander recently renounced any interest in the NSA having a lead role securing non-defense governmental networks.¹² Instead, procedures should be developed for ensuring that whatever expertise NSA has in discerning attacks is made available to a civilian agency.

¹⁰ Resignation letter of Rod Beckstrom, former NCSC director, <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>, March 5, 2009.

¹¹ Commentary by CDT Policy Director Jim Dempsey on Bush Administration cybersecurity initiative, <http://is.gd/piNP>, May 14, 2008.

¹² Declan McCullagh, NSA Chief Downplays Cybersecurity Power Grab Reports, *CNET News*, http://news.cnet.com/8301-13578_3-10224579-38.html, April 21, 2009.

Some have suggested that a new cybersecurity office should be established in the White House, and that this office should be tasked with overseeing the entire program. They argue that only the White House has the authority to direct agencies to do what needs to be done to protect their own systems. However, such an approach risks politicizing the cybersecurity program. Moreover, as Senator Susan Collins (R-ME) recently pointed out, putting the cybersecurity program in the White House would mean less Congressional oversight and more secrecy.¹³

In thinking through a proper organizational approach, it is helpful to separate responsibility for developing cybersecurity policy from responsibility for cybersecurity operations. In our view, the White House role in cybersecurity should be to set policy and direction, and to budget enough resources for the program. This could be done through a newly established White House office, rather than in one under the National Security Council, whose activity would be shrouded in secrecy.

While some have proposed moving primary responsibilities for cybersecurity operations from the Department of Homeland Security to the Department of Commerce, we do not believe that the case has been made for such a disruptive move. In short, the problems that plague the program won't be fixed by moving them from one governmental box to another.

The lead for cybersecurity operations should stay with the Department of Homeland Security, and the NCSC should be provided with additional resources and high-level attention. DHS Secretary Napolitano recently named Philip Reitinger as Deputy Undersecretary of the National Protection & Programs Directorate. Reitinger is the former Chief Trustworthy Infrastructure Strategist at Microsoft, where he helped protect critical networks. He is well qualified to lead cybersecurity efforts at DHS and to make DHS the government-wide lead.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. The key is to acknowledge the substantial differences between the Internet and other critical infrastructure systems, and to tailor solutions to the systems that need protection. Effective cybersecurity measures intended to increase security of the communications infrastructure need not threaten civil liberties. As a general rule, market-based solutions instead of governmental mandates should be favored for private infrastructure systems. The Subcommittee on Communications, Technology and the Internet can play an important role in implementing these approaches to cybersecurity and in keeping the Internet the engine of innovation and robust discourse that it has become.

¹³ Letter from Senator Susan Collins to DHS Secretary Janet Napolitano http://www.cdt.org/security/20090324_collins_ltr.pdf, March 24, 2009.

Mr. WEINER. Thank you very much.

I would like to begin the conversation looking at, first, in some, as much as we can do in English, some of how the big stories of the day have emerged. When we read in The Wall Street Journal and elsewhere that computer spies have breached a fighter jet project; when The New York Times reports that a vast spy system lures computers in 103 countries, walk me through a little bit about, and while you can't answer with certitude, a little bit of how we suspect these things have happened and why it is that the cat is a few steps behind the mouse on these things.

Mr. Kaminsky, you can start. You can choose either one of these. Walk me through about why this is more complicated than simply saying, let's just read some code, close some back doors and solve this problem.

Mr. KAMINSKY. I would say there tend to be two main ways that attackers seem to be getting in. There are more, but I will go with two. The first way is that the software that is exposed on the Web for remote access, remote management, remote just data collection, while operating systems themselves have gotten significantly more secure over the last few years, the actual software that is exposed that drives Web sites tends to be homegrown and very poorly audited.

So a very common technique that attackers use is what is known as sequel injection, where they actually communicate with the Web front end and messages are sent to the database back end. And the messages, unfortunately, are insufficiently sanitized or cleaned, and the database is caused to run arbitrary attacker software. That is the most common implementation flaw.

The other method is what I referred to earlier in my talk where I was talking about authentication techniques. According to the Verizon business report, 4 out of 10 of the times when they saw an actual compromise occur, they actually found that there was remote management—remote management there specifically for third parties, for third-party vendors, using passwords that were either known or could be easily guessed. So we don't have the exact details, or at least I certainly do not have the exact details on how the joint strike fighter data was lost. But in terms of what was lost from server side, you will see either compromises on the Web site or compromises on remote management through default passwords.

One third case which should be brought up is that we do have issues with actual desktops and browsers themselves, where an individual desktop inside of an organization will be compromised through the Web browser through what is called a drive-by download, and that drive-by download will cause that individual host to be a jumping-off point for an attacker to then attack other assets within the organization.

Mr. WEINER. So that then leads us to Mr. Clinton's testimony that if you know these things, and these things thankfully keep you in business, Mr. Kaminsky, does the panel agree—maybe Mr. Kaminsky, you want to expand upon this—but if an overwhelming number of the attacks happen in a certain prescribed way and that if there are certain steps you can take to protect yourself, and I think Mr. Clinton's testimony was 80 to 90 percent if you follow certain protocols; is this a problem people have, people being sloppy

and what we are looking at is we figuring out ways to make them less sloppy?

Mr. Clinton, is that a fair summary of at least that portion of your testimony?

Mr. CLINTON. Thank you, Mr. Chairman.

In part. I wouldn't say that it is necessarily people being sloppy, but there is some sloppiness involved. I would go up a level.

First of all, I would never dream of getting into a technical discussion with my colleague on the right. I will just accept everything he says as true.

I would operate at a different level. He can tell you in great detail why a particular attack happened. But once we have plugged that hole, the attackers are going to move to another hole. So while we can, you know, patch various holes in the Internet, they are going to continue to find new holes.

What we have to do, in our opinion, is change the system. We have to change the economics of it. The reason we don't have all of these things patched in the first place is because users don't like security. It makes it harder to use, costs money; businesses the don't like it. What we have to do is change the system, so that instead of people trying to view cybersecurity as a cost center or a bother, they have got to view it as something they want to do so that we can change the economic dynamics of it. And that is what we are arguing for.

So it is certainly true that if we had the right incentives, people could fairly, quickly, and easily, according to the research and the CIA, could reasonably mitigate enormous percentages. I am not sure if it really is 90 percent, but that is what several studies say. If it was 80 percent, it would be an enormous advantage. And we would have to do this on a continuing basis. Once we put up a system of—once we implemented all the best practices that the Verizon study suggests and we were able to stop this 80 percent, we would have to continue to work on that system because the attackers are going to say, okay, they have plugged all those holes; we are going to go after some others. So we have to do this on an ongoing basis, so the system has to continually grow because the system continually grows and changes.

Mr. WEINER. Doesn't this face the conflict, then, that it is in Google's interest to patch things that attack Google. It is in Verizon's interest, notwithstanding this industry-wide report, to attack things that attack Verizon?

Mr. CLINTON. Right.

Mr. WEINER. Where does the system-added conversation happen?

Mr. Nojeim raises concerns about we the government entering into that field, but where should that conversation happen where someone is thinking about the system-wide protection? What is the recommendation of the witnesses on that?

Mr. Kaminsky.

Mr. KAMINSKY. Too much of this discussion happens in the context of, how can we apply more pressure to people? How can we push them? How can we force them, or at least in the nicest way, how can we incentivize them? I don't think enough of the discussion happens around, how can we reduce the cost of delivering a secure solution? Users don't like security because security is too ex-

pensive and too difficult to deploy. Some of the most expensive failed information-technology projects in the world, we are talking in the \$100 million scale and up, have been in systems that have attempted to do cryptographically asserted authentication.

A major role that government can play here is in giving all companies, giving Google, giving Verizon, giving Microsoft, giving us all one shared base that we can start building trust on. The Department of Commerce is doing an enormous amount of painful and thankless work to get DNSSEC to be something that can actually work with a central root of trust. The advantage to this is not just that we fix DNS. It is that we take so much of security technology, which has been a lot of promise and not as much user-opting-in as we might like, to make this stuff inexpensive enough so that it is actually something that can be deployed. People want security, but they want their systems to work after, and they don't want their costs to explode. DNSSEC can help that.

Mr. CLINTON. If I could just quickly, Mr. Chairman. And I would agree with what he said, but to get to your broader issue of, how do we get everybody to do this, it is because everybody has got to see some sort of benefit to doing it. I mean, the problem that we have is, this is a joint system, and the vulnerability is distributed. And they may be trying to get to—China, for example, may be trying to get to the Pentagon. They don't attack the Pentagon directly. They don't even attack Raytheon, that is linked to the Pentagon. They attack Raytheon's subcontractor, and by getting to Raytheon's subcontractor, they get to Raytheon, and through that they get to—so we have to get out to that subcontractor. And the subcontractor in the current system says, well—the Pentagon says, we will give a contract to Raytheon, and they will enhance their security, which they do. They have very good security. And we will tell them to enforce it on the subcontractor. So Raytheon attempts to do that. So the subcontractor says, I am sorry, it is just not worth it for me. I don't want the business. I mean, this is like 5 percent of my business. I am not going to change over my entire information security system. They walk away from the business, which is bad from everybody's point of view. What we are advocating is, we need to have an incentive in place, a small business loan, an insurance benefit, something—there are lots of them—so that the subcontractor now wants to keep his or her security completely up to date. So that we have an incentive for Raytheon that is a procurement contract; we have an incentive for the subcontractor, maybe you know, the ability to get an SBA loan or a lower insurance rate, and so that everybody has—we need a system-wide set of incentives, and the incentives are going to be different for different people. This is not a one-size-fits-all world. We have to stop thinking of it that way. We need a network of incentives to address a network security issue.

Mr. WEINER. It is puzzling, though, it is puzzling though that we need to offer incentives for a government contractor of Raytheon to do what is intuitive, which is to not share terabytes of information on the Internet with hackers. I am not quite sure that the—I mean, it strikes me that this gets back to the question and answer; how do you make sure that the silos of security extend—I mean are systematic?

Mr. Joffe.

Mr. JOFFE. Thank you, Mr. Chairman.

There are a couple of fundamental things to think about here. We talk about incentives. There are some fundamental issues. When it comes to incentives, one of the key things that I find when I talk to large corporations that have issues is, they say, well, what is in it for me? And that is really the thing that should drive the incentives. The incentives will be different, but as long as you can show someone what is in it for them.

One of the problems we have now is that there are—the issues could affect so many parts of the world and so many parts of the commercial world that people say, why would I step up and fix my part of the problem if other people aren't fixing their part of the problem? Someone else will do it. It seems to be a driving theme in most of the meetings I end up having.

And until I can point out how it affects someone specifically, they really say, not our problem. People don't think about it as being their problem.

The second thing is that the bad guys are as good as we are. One of the problems that we are facing and doesn't seem to be sort of dealt with much is that the people behind most of these attacks are as good as we are if not better. For some other reason, it almost seems like the bad guys are us. The level of sophistication, the things that we see, for example, in Conficker using, you know, certainly state-of-the-art and best-of-breed techniques.

If I was a university professor, grading something like Conficker.E, it would have a very, very high grade. They have done everything right. We don't seem to be able to do it. Maybe it is because you go to the typical large government contractor, and there are 50,000 or 60,000 people who are involved with software development in some way. It seems to be very difficult for us to be able to control that, and there doesn't seem to be enough of an incentive overall for the companies to take a holistic approach until you see the front page of the Wall Street Journal. Then, all of a sudden, everyone wakes up.

Finally, there are two different ways that this happens. One of the ways—and I don't know—obviously, I know nothing about the Joint Strike Fighter issue. But in many cases, this is determined breaches by humans where someone works away at finding the problem. They have all the time in the world. They have a lot of patience, and they work their way through breaking into a system, including using social engineering. A lot of things that have been found have been as a result of social engineering. The issue with USB drives, for example, which not only was an issue for the Federal Government but is an issue with Conficker. One of the major reinfection vectors we see now is people cleaning their machines off, but before they do that, they copy their key documents onto a USB dongle. Clean the system, rebuild it, go through all the effort and plug the dongle back in, in order to copy their key documents across, and they are getting reinfected. That is what we are seeing with Conficker.

The first way is human breach. The second way is, a lot of the attacks aren't as a result of conscious attacks. You get something like Conficker or Torpig or one of the large botnets. They go out

there and become like vacuum cleaners. They do their work in an automated process. We don't even know in many cases how systems got infected because they theoretically aren't connected to the Internet. The mystery behind the botnet, what they are able to do is sit and look at the net result of the vacuum cleaner.

If you think about this, there are over 4 million machines currently infected, we think, with Conficker. We don't know where many of them are. We see a lot of them checking but not all of them. If someone behind that botnet wanted to, all they would have to do is perhaps use it as a giant search engine, basically say, show me any document or give me anything that has somewhere on the hard drive the word "nuclear," the word "blueprint," the word "trigger"; come back and find it for me. And all they have to do is sit back and wait. And over the course of a short period of time, those 4 million machines will look at their local drives and because, as we now know, many of them are actually sitting behind corporate firewalls, they will then examine all of the shared drives.

They are basically no different than the human sitting behind the computer that is infected. They will look at all the shared drives and examine all of the documents looking for that word. Very little work. Somewhere or other, out of maybe a token Congress IP address that maybe is even connected to a home modem, they will find the right set of documents, absorb those, send them back to the miscreant. And before we know it, you have the front page of the Wall Street Journal.

Mr. WEINER. Mr. Nojeim.

Mr. NOJEIM. Just a couple of thoughts on this. One is that the bad guys in the fighter jet incident didn't get the best information. They didn't get the most sensitive information. That was on a separate system. And maybe one answer is that, at the time of procurement, the government better describes what has to be on a separate system that is not connected to the Internet. Procurement can be a very powerful tool in your war chest, if you will, for dealing with this problem.

Another thing to think about is that Raytheon is probably protecting its systems in the way that it thinks is most appropriate. It has got people whose job is to do that, and they are acting in the way they think is best. If the government believes that they should be acting in a different way, that additional security measures should be in place, then it should be up to the government to pay for those additional measures and the compensation could be through credits, could be through tax credits, or it could also be through a procurement provision so that you get extra money if you take extra steps.

Raytheon may not have protected that subsidiary in the same way that it protected other more sensitive systems. If that subsidiary needs to be protected, then maybe Raytheon doesn't get the contract. And if it does get the contract, maybe the contract also pays for such protections.

Mr. WEINER. Well, let me use that as a jumping-off point to some of the other threats; that some have been realized, some have been unrealized. Can you talk a little bit about the danger of expanding the use of smart metering on our electric grid and the vulnerability that it extends to the notion that our electric grid might be vulner-

able. Some of our colleagues on the Energy and Commerce Committee talk about empowering FERC to regulate these things further. Let's think about, not the challenges of the past, but let's think about some of the things that we might be vulnerable to.

The electric grid, as I understand it, by and large is not susceptible to a wide-scale attack because it is by and large not attached to the Internet in a large measure. Is it a source of concern to any members of the panel that our energy infrastructure might be susceptible to attack?

Mr. Kaminsky.

Mr. KAMINSKY. There is an old joke from the NSA which is that all networks are connected; it is just a matter of how fast.

The energy industry is, on the one hand, completely different than the rest of technology and, on the other hand, no different at all. The 1990s saw a tremendous increase in our use of personal computing technologies and information technologies to, quite frankly, make work more efficient. The energy industry has not been immune from that.

One of the technologies that we have seen spreading, at least in recent design, has been an ability for the actual power meters to communicate with one another, for them to create a peer-to-peer mesh as one meter speaks to another meter speaks to another meter. This technology is being done by people who, frankly, have not had to deal with the last 10 years of attacks. And on analysis, we have seen these meters actually able to be compromised remotely.

Where we are today with the energy industry, which is there are a lot of information systems, there is a lot of communication going on, there is a lot of gear that has trouble dealing with attackers today, and the only thing preventing pretty widespread attack is a lack of connectivity. With connectivity growing more and more, that is a temporary solve. The future, the future of widespread meter-to-meter communication based on the evidence that I have seen thus far does have me concerned. I would like to see more security for those meters.

Mr. WEINER. And are there steps that can be taken? Or is the technology of the smart grid too new to have best practices in this field?

Mr. KAMINSKY. I think we know how to make secure devices. I don't think that that is the problem. I think the problem is that the devices, as they have been made, have not been made with that knowledge. So this would be the sort of thing that certification and independent evaluation would improve. We know how to do it. It is just the devices that have been built thus far, when we actually test them, they tend to fall over.

Mr. WEINER. Mr. Joffe.

Mr. JOFFE. Thank you, Mr. Chairman.

One of the biggest problems that we face is that the Internet was never designed to do the things that it is doing today. There are control systems. There are systems that were never designed to be on the open Internet. But the open Internet, one of the great values is the fact that it allows you to communicate fairly cheaply and fairly easily with other computing devices.

Traditionally we used point-to-point connections. There are home-monitoring devices for people who have medical conditions that traditionally made use of a dial-up line and a dial-up modem to communicate that to a doctor's office or a hospital. And people realized very rapidly that if you made use of the Internet, the existing cable connection or DSL connection, you could have much faster, much more reliable connectivity. So the devices were moved on to the open Internet without understanding from a design point of view that, at that point, the security requirements were different.

The same thing is happening in the power industry. The power industry devices are being developed by not necessarily people who are in the power industry but people who are in the computing industry. So they develop devices and the device is then used by the power industry who are used to a closed network. But by its very nature, those home devices, the smart meters are going to have to rely on the open Internet. If they made use of the technology that the power industry was used to, which was point-to-point secured connections, or in fact the same techniques that existed in the phone industry, there wouldn't be an issue. But there is a disconnect between them. Perhaps it is an educational issue where you have the wrong groups of people getting the right training.

As Dan had mentioned over there, we certainly know that security is an issue. But the people that build the devices, when they first design them, don't think about security first; they think about functionality first. And security is an afterthought, and it really shouldn't be. It should be embedded in the system.

Mr. WEINER. Mr. Clinton.

Mr. CLINTON. I agree with Mr. Kaminsky and Mr. Joffe both with regard to the fact that we can build more secure devices, they will be more expensive. But the point I want to add is we also have to operate these systems better.

The single biggest vulnerability that we have is not technical at all, it is the insider threat. Depending on which study you read, a third to half of the problems that we have are from people on the inside. These are people with keys to the technology. You can have the best technology in the world and the best security in the world, but if you just fired your IT guy, and he has put in a back door and he wants to come into your system, he will do it. That is 30 to 50 percent of the problems.

So we not only need to have good technology, we need to have incentives for people to use the technology. Again, this is a system-wide problem. It involves technology and human resources. It involves the economy and legal compliance. It involves a variety of things. It is not going to be fixed when somebody comes up with a new device.

Mr. WEINER. I want to talk about a couple more emerging threats, but before we do, I think we should touch on Conficker and what the state of play today is. It is exactly 1 month from April 1st, the day Conficker was supposed to bite. There have been some things that have happened since then.

Who would be best to tell us what is the state of play with Conficker right now, whether it is still something people should be concerned about; and more troubling to a layman like myself, why

is it that we literally have the code right there in front of us and it is such a vexing issue? What does it say? What is it doing? It seems to me there has to be at least someone who can read it, who is at least as smart as the guy who wrote it and say this thing is going to turn all microwaves on.

Mr. Kaminsky, can you give us as best you can in English language, and I know how difficult it is when you are dealing with these technical matters, where does it stand? Are we going to get up to Conficker.P? Tell us whether we are learning anything. Just give us an update on where we are with that.

Mr. KAMINSKY. Not a problem.

So it used to be that if someone wrote malicious software, they wrote it, it was out there. You could analyze it and tear it apart and figure out exactly what it is and what it is going to do. That is how things used to be.

The new generation of attacks are not about it does what it does, and it can't do anything more. The new generation of attacks, as Mr. Joffe said, are all very much about go back to the attacker and find out what would you like? Would you like me to search for documents? Would you like me to search for updates? Would you like me to do anything you can possibly imagine?

That is what has made things difficult. Conficker is quite possibly the single most analyzed piece of software in the last 10 years; but we can't tell you everything it is going to do because we don't know because the attackers have not issued the commands or have not released the actual software in a general sense. It always goes and retrieves updates.

What made Conficker special, and what continues to make it special, is that it is actively being maintained and actively defending against the security community's effort. That does not mean that the security community has been lost and unable to do anything about it. We have had entire months of restricting Conficker's ability to update itself and manage itself. Through the public-private partnership of the Conficker Working Group, Conficker.B's entire update strategy was pretty tightly constrained. That is what ended up leading to their need to do an April 1 date. On April 1 they moved from the defenses that were successful in February and March to what we were unable to defend against in April. Technical terms: They moved from using 250 domain names a day, which we could register, to 50,000 domain names a day, which would be too difficult to block.

The state of play as it is today is we have very, very good tools for quickly scanning networks, identifying where Conficker is so that it can be quickly cleaned.

In order to actually get rid of Conficker, it was never, at least in my perspective, about how do we pressure people into doing it, because pressure will only go so far. It was how do we make it less expensive, less difficult, less time-intensive to actually find this on networks.

Since a little bit before April 1, we have had fantastic tools for sweeping networks to find this. Now it just is a matter of people running those tools and cleaning it off their networks. There are still a few million nodes, but it is going down every day.

Mr. WEINER. You said that Conficker had the ability to go from 250 to 50,000 with an order. Can it keep ahead of you, or are you closing more doors than it is opening as it goes day by day?

Mr. KAMINSKY. I will yield time to Mr. Joffe in a second, but I will say that I don't think that we will be able to stop the Conficker authors from sending updates. I do, however, think we will always be able to detect the Conficker-infected hosts. The Conficker authors are doing a lot to try to defend themselves from being found and caught.

The place where I think we have a sustainable advantage is it appears no matter what they do, we can always find them so we can determine we need to clear them.

Mr. WEINER. Let me ask you this: This being the new state of the art in these things, are other hackers and other troublemakers able to look at the Conficker virus and say, huh, that is a cool way or a vexing way or a troublesome way for us to do our business in the future? Is there now out in the world this new model which is going to mean that the cat and mouse game is going to extend to other hackers who are going to use the same device?

Mr. KAMINSKY. Honestly, I think that is a fair statement of the situation. One person has gone ahead and taken a lot of the worst practices, as opposed to best practices. Someone has actually demonstrated the worst practices for how you make something that doesn't just compromise a network today, but has a sustainable advantage, an update advantage. So I do think that we will see more things of that type.

Mr. JOFFE. Mr. Chairman, there is an interesting thing to note about Conficker and April 1. Most of the press saw April 1 as the day when Conficker would suddenly erupt. It was going to be like Y2K.

We knew already that we had been able to disassemble a fair amount of the software. We knew that April 1 represented one thing only, which was a change in the mechanism that Conficker was going to make use of.

Up until then, as Mr. Kaminsky mentioned, we had been able to control, or we thought we had been able to control, the spread of it. They changed the mechanism on April 1. But on April 7 and April 8, as you pointed out, it went to Conficker.E. Conficker.E did two things. The first thing it did was it updated Conficker.D to a new mechanism for both spreading and communicating.

The second thing that it did was it enabled the download of another piece of software called Waledac, which is another form of malicious software. It enabled the downloading and installation of that, with some very interesting pieces to it. We don't know if the authors of Waledac are the same as the authors of Conficker, but it is very clear these are businessmen.

What Conficker seems to have done is downloaded Waledac, but done it for 2 weeks only. It is a very interesting process. It is almost as if the authors of Conficker rented the use of Conficker to the authors of Waledac to download Waledac, and after 2 weeks to delete it.

What we have been able to see from disassembling some of it, I think it is on May 3 or May 5, any installations of Waledac done by Conficker will be deleted. These people are very, very smart.

One of the things you asked: Don't we know who is behind it? Can't we interrupt it? The cryptography that is used in authenticating between the controller and these machines is so sophisticated; in fact, it didn't exist in the public. The particular thing that they are using, which is something called MD6, was actually submitted for the NIST competition for the new cryptography that will be sort of authorized for the government networks in 2013. They had used this 5 weeks after the submission from Ron Rivest. They had this in place and were using it. It uses a level of cryptography that, as far as we know in the private world, there aren't enough computing cycles to be able to crack that in any way. It is being used to authenticate the updates.

So we can see the software, and we know the machines are infected. We can disinfect machines with a lot of effort. But what we cannot do is something people have asked: Isn't it simple to just act as if you are the controller and tell the worm to disable itself? The worm doesn't listen to us because we don't have the right signature. We don't have that crypto capability. They are doing a much better job with cryptography than we are.

Mr. WEINER. This is detective work, but is one of the emerging theories that what Conficker is is a delivery device for or a distribution device for other spammers or hackers or malware delivery? Like we will rent it to you. This is a great moving vehicle. For 2 weeks we will let you use it, and we are going to rent it to someone else for the next 2 weeks, and this is just the way that it gets around.

Mr. KAMINSKY. It is all about monetization. It is about what can they do to make money from their millions and millions of infected nodes. In this case, they have made money by renting it to other people who have their own strategies.

The one thing I would really like the committee to be aware of is there is no reason what Conficker does to one company is the same thing that it does to another company. There is no reason what Conficker does to one computer is going to be the same as what it does to another.

Mr. WEINER. It is an operating system?

Mr. KAMINSKY. It pretty much is. It is a remote-control mechanism, and you can make an individual host—one host do one thing and another do another. If that is the best way you can make money, go right ahead.

Mr. WEINER. I want to touch on one or two more potential horrors of the future, if not the present. One is the proliferation of mobile computing devices, cellular devices and wireless devices. Is there a reason why we haven't seen—and maybe we have, but not in the same highly publicized way—the wide-scale hacking of those devices? More computing is now going there. More communications are now going to handheld devices. Is this the next frontier of cyberwarfare? Have the cybersecurity threats already begun there? Are there reasons why it is less able to do because the technology is not as sophisticated as the network? Tell me if there is reason to believe that could be a vulnerability of the future.

Mr. KAMINSKY. Mobile phones have become operating systems. They are quite a bit more complex than the computers we were using back in the 1990s.

The reason we have not seen attacks against them in significant count thus far is not because they are more secure. Any engineer who has actually taken a look I do not want to say has run away screaming, but has certainly found themselves concerned.

The bad guys figure things out, but not immediately. We are basically enjoying something of a time lag in between when there is awareness of being a problem and when the hackers have built up the expertise to be able to exploit it. This will change over the years, mainly because at the end of the day, all of the things that we have managed to really clean up in operating systems and really fix up there, not all of them have made it into the mobile phones at this time. That is just the reality of things.

Mr. WEINER. Mr. Clinton, do you see the sense of the infrastructure limitations and the infrastructure vulnerabilities have been addressed? And I guess one reason it would be easier to protect is there is a finite number of wireless carriers with a finite number of technological pinch points.

Does it seem like the industry on the wireless side has taken these best practices and have done what you described as the need that 80 or 90 percent of the attacks can be protected if you make best practices?

Mr. CLINTON. I really don't know if I can say that about the wireless industry; although generally, the major carriers do a pretty good job.

The core problem, though, as I understand it, not to delve too much in areas that Mr. Joffe and Mr. Kaminsky can answer better, the Internet is really inherently insecure. The core protocols that the Internet was built on were built 35 years ago. Nobody was thinking about security. They are pretty much completely insecure at their core, which is why we have a patch system to solve these problems. As long as we are using these core protocols, which are basically the same protocols we are using on the mobile systems now, they are going to be insecure, too.

The only thing that I would add here is, I think we need to be careful by focusing just on kind of the high-profile issues like Conficker. I mean, I do a lot of speeches on this and sometimes go out and people say, I used to hear a lot about what you do. There was the Love Bug and Blaster; I don't hear about those things, Conficker notwithstanding. I guess you guys solved that.

Of course, that is not the case at all. We have simply moved largely from an era—an era, 5, 10 years ago—5 years ago, where the hackers were focused on large-scale public demonstrations of their ability, to an era where we are really focused on designer malware, and the goal is not to show what you can do, it is to steal money.

So we are really not sure how much stuff is out there. A lot of the problem with extortion is people are simply buying silence.

I would caution against just thinking, if we can solve Conficker kinds of things, we have solved this. I think it is harder than that.

Mr. KAMINSKY. I wanted to clarify. There is at least one mobile platform which has been paranoid for years and years, and I can say this because I know the years. The BlackBerry Research in Motion guys have worked for as long as I have known them to build

a secure mobile platform. At least in that case, I can say people have looked at it, and their stuff is pretty good.

In fact, a lot of people kind of shrugged their shoulders at the “ObamaBerry” controversy. It is not like President Obama is the first person to ever be putting sensitive information into their BlackBerry.

Mr. WEINER. Mr. Kaminsky, you don’t do any consulting work for BlackBerry, do you?

Mr. KAMINSKY. No.

Mr. WEINER. I just wanted to make sure that I didn’t get some Apple lobbyist complaining or anything.

Mr. Joffe.

Mr. JOFFE. One thing to remember is that mobile devices used to be telephones, but they are now becoming much more of a computing platform. We go after Microsoft a lot in terms of their operating system. That is not necessarily where the problem is. It is the applications that people download and use on those devices.

We are beginning to see a move towards mobile payments, for example. One of the things that you have to be very careful about is when we look at the mobile payment applications, they sit on top of the operating system, on top of the phone. They have to be looked at on their own because you can have the most secure platform you want. If you have an application that enables problems, it doesn’t matter how good the operating system, the application itself would be insecure. That is where the problems, most of the problems that we have seen today, are coming from.

Don’t think of it as a wireless device. It is nothing more than an existing computer, and it is just as vulnerable and has to be looked at very carefully in the same way we do on regular computing devices.

Mr. WEINER. Finally, on the challenges that we face, how do we know that a router manufactured in China doesn’t have some listening ability built into it for Chinese Government officials? Or some computer chip that is made doesn’t have a circuit switch that permits anything on that computer to be, with the right command, listened to or going to the right Website? How do we know that hacking in is not the issue, that building in might not be the issue?

Mr. Clinton, you are nodding the most, so why don’t you start.

Mr. CLINTON. We are very concerned with this problem. My organization started 3 years ago in conjunction with our partners, Carnegie Mellon, to take a look at exactly this problem. And basically, to put it in short form, I think we have come to the opinion that we need to learn how to build secure systems, understanding that some of the parts may be insecure.

We do think, and we have amended our statement, a fairly extensive additional piece of work that we did with Carnegie Mellon and Scott Borg at the Cyber Consequences Unit to move towards developing a framework so that we can put in an extended system of protections so that we can secure the IT supply chain, which is inherently globalized, is going to stay inherently globalized, and is going to be built in part by people who we don’t know. They don’t have a Social Security system in India. But we can put in, we think, by using a fairly systemic framework that we have tried to begin the articulation from in some of our additional comments,

which we also supplied to Ms. Hathaway, a system where we can again change the economics so that we can make it in our best interest and our suppliers' best interest to understand that it is in their best interest to keep these systems truly supplied in a secure fashion, rather than allow them to be counterfeited or in some way hurt.

The one thing that I would say in addition to this is that we try to take a risk-management approach to this. So while we are very secure, we are very worried about the supply chain. This is a problem that is generally not a big problem, we think, for industry. The reason is it is usually easier and less costly if you are going to attack Bank of America to attack it through software or one of these traditional hacks. It is much harder and more difficult to do it through a supply-chain attack by putting something in the computer.

However, from the government's perspective, this is an extremely serious problem, because if a weapons system could be infected through a manufactured attack, you can't detect it. You don't get rid of it when the software is there. And the chances—it is absolutely possible to put in a back door or a Trojan horse, a logic bomb that will stay there and not be activated until we launch a weapons system, and then the weapons system could either not work or turn around and go against us. So it is a very serious problem.

And if you are a nation state, and you are thinking of weapons of mass destruction, then a supply-chain attack could become very attractive to you, much more attractive to you than if you are just trying to steal credit card information.

Mr. WEINER. Let me pick up on something you said. It is easier not to do it on the supply chain. If you are a nation, if you are China, and you have a lot of manufacturing going on within your boundaries, and you have the ability to manipulate branch managers, could it also be a source for our counterefforts? One thing that we have that the rest of the world envies, we have the technological expertise, and we have a lot of the companies that manufacture these parts within our walls. A lot of the chip manufacturers are U.S.-based companies. Why couldn't we install things on these chips to make them—if we want to throw a switch, as we tiptoe into Mr. Nojeim's area of expertise, why don't we install a switch that goes into these routers that lets us shut them down if they fall into the hands of Iran or a foreign power? I mean, it seems to me that it might actually be in the interest of the Chinese to be doing it to us and the interest of us to be doing it to the Chinese, no?

Mr. CLINTON. On the weapons system, I think this is a big problem. In terms of the economic sort of stuff that we have been discussing here, the personal identifiable information sort of thing, one of the things that is a good thing about the globalized economy is that it is, frankly, not in China's interest to have lack of confidence on the Internet or to undermine the American economy. They are big investors in the American economy, so it is probably not so much in their interest to do that.

But if you think of it in a military sense, I would not be shocked to hear that we have people who are thinking about doing it offensively from our point of view. And certainly the expectation is that some of our opponents are thinking about doing it from their point

of view, and that is why this kind of framework that we have suggested in our written testimony needs to be developed a lot more.

Mr. WEINER. Mr. Kaminsky, if I were to manufacture a router that had a piece of code or something built into it, and you had enough time to look at it, could you find it?

Mr. KAMINSKY. It would be difficult. The reality is attacks at the level where the actual hardware has been corrupted in the first place are very, very difficult to find. The researchers that Mr. Clinton spoke about at Carnegie Mellon University have done some preliminary work in attempting to detect these actual back doors, but at the level where it is baked into the circuitry, it is actually very difficult to find.

What is not difficult, however, is if you are the one doing the baking, you can pretty much make hardware that no matter what software is run on top, you can ultimately get an exploit into that operating system. So whatever operating system, whatever software, if you control the underlying hardware, you control the underlying logic, you can make a back door, and you will control that system.

Although it is true that we have a lot of very creative companies in the United States, the reality is a lot of the development of both hardware and indeed secure software happens outside the United States: China, India, Taiwan and so on. That is just the reality of the market as it is today.

Mr. WEINER. That sounds like a pretty frightening conclusion, so let's start to end the conversation today talking about the conflict that is going on now within the Obama administration about who should be in charge of this and what they should do.

It seems to me, Mr. Nojeim, that there does seem to be sufficient risk that we do want to give the tools to government to be able to—if the risk grows too big too fast to critical infrastructure, to our country, to a weapons system that might be used against us, there needs to be some check on the basic ethos of the Internet being a completely democratized, fairly loose-knit organization. Some have taken that argument to the extension of saying, all right, the supervisory/governing agency that should be at the top of the organizational chart of cybersecurity should be an intelligence or defense agency. What do you say?

Mr. NOJEIM. We don't think that is the right approach, and there are a few reasons for that. And the Agency we are talking about is the National Security Agency, for the most part.

NSA has a role, I think, in protecting classified government systems, military systems. But it is not necessarily the case, and it probably isn't the case, that the NSA would be the best entity to protect a private system that is not in the classified realm, it is not in the defense realm.

Let me illustrate it this way. If I am Mr. Kaminsky, and I am working for Microsoft, I might know my systems better than anyone else would know them. The fact that the NSA has experience in penetrating other systems of foreign countries abroad doesn't necessarily make it the best entity to protect systems. Also, the NSA, it wears two hats. Those different roles tug in opposite directions in the cybersecurity area.

One, it is charged with breaking the codes of foreign governments and penetrating their systems, finding vulnerabilities. But if it was given a lead role in cybersecurity over private systems, that role would conflict with the need to patch up systems that are being used in the United States. Sometimes it is exactly the same system.

So if NSA finds a vulnerability abroad—

Mr. WEINER. Meaning that you wouldn't want to tip off a foreign power that you have spotted this weakness because it might exist in our own?

Mr. NOJEIM. Because they wear these two hats of finding the vulnerabilities, and then wanting to plug vulnerabilities in the same software that is on our systems, I think that is a very difficult thing for them to handle, and it probably makes them an inappropriate leader.

I should add that the head of the NSA at the RSA conference just a couple of weeks ago said, we don't want this lead role. We don't want to be doing that.

Mr. WEINER. I think there was some element of kabuki dance going on there.

I think we now understand that one of the reasons that this 60-day review has dragged on, and I don't think there has been an appointment of a chief technology officer, one of the reasons is that they are legitimately hung up on this. Any advice? Is there a need to have all of these disparate agencies that deal with cybersecurity? Is there a need to have them under one umbrella? There does seem to be consensus among folks who have looked at this that there is too much interagency back and forth, elbow throwing, and planning on who is responsible for what that doesn't lend itself well to a true emergency response.

Do you have any advice to offer the President, Mr. Clinton?

Mr. CLINTON. First of all, we generally stay away from this because, being a private-sector organization, we are always telling government, don't micromanage us. So we generally try to stay away from offering advice.

One of my board members would answer this metaphorically by saying if the cybersystem were a soldier on the battlefield with an open wound, and the Intelligence Community were the doctor, the Intelligence Community's approach to that would be to look into that wound and say, my, isn't that interesting, as opposed to, fix it. And we need people who are going to fix it, not try to exploit the vulnerability.

The one piece of advice that we would offer to the administration is regardless of whether you locate this person at the Department of Commerce, such as the Senate bill would suggest, or DHS, where it is supposedly now, or NSA, the important thing is not where it sits, but that you do have an individual or an organization, it could be a group of individuals, who have actual control from the government's perspective. That individual needs to have budgetary authority and the ability to oversee the other organizations. It can't be just kind of a figurehead position.

So it is less important to us where that person sits, although we tend to think it should be somewhere within the White House structure, but that person actually have the ability to do the coordi-

nation. And we also think that government's first role here is to get government's house in order rather than try to figure out how they are going to deal with the private sector, which is why I think the model we have suggested, which is a collaborative model, is something that we would ask the committee to take a look at.

Mr. KAMINSKY. There is a scenario that I think has been useful for explaining to people just the scale of problem that we have.

Consider a situation where a major top 10 Website is broken into, not directly but through their ad network. The advertising network is made to deliver an exploit for the Adobe Acrobat document software. The documents are loaded. They cause code execution on anyone who goes to that Web page. The code loads up a botnet. That botnet is used to do two things. First, it sends banking credentials from the infected host to the attacker. Second, it floods various Websites on the Internet with malicious traffic in a desire to force an extortionary attempt to be successful.

Whose fault is this? Is this the fault of the top 10 Website? Is it the fault of the ad network? Is it the fault of Adobe? Or is it the fault of Microsoft for writing the operating system, or the user for using the operating system? Is it the fault of the bank for having credentials at all? Is it the fault of the people who pay extortionary prices?

The fault is the bad guy. The bad guy caused this, and everybody else has a natural alliance against that bad guy.

The problems that we are trying to solve are smeared across company boundaries, individual boundaries; and, indeed, are smeared across the public-private boundary. I agree with what has been said earlier. I don't think that I am qualified to know who or where there should be authority, but there actually does need to be a coordinating authority across all of these disparate actors to guide the public-private partnership towards actually fixing the scale of problems that we face today.

Mr. WEINER. Mr. Joffe.

Mr. JOFFE. Thank you, Mr. Chairman.

From my point of view, I, like Dan, come from the geek side of the house, and we don't play in politics and are down in the trenches. The only way we are going to solve this is by, first of all, acknowledging there is an issue, which is exactly what the White House has done with the 60-day review process, the other hearings that have been heard on the Hill, and this hearing. The fact that we are having this kind of hearing, this is remarkable to us in the technical world. Eight, nine years ago, none of us would have been seen up here unless we were involved in something else. So it is really important that there are hearings and we acknowledge there is a problem, and acknowledge that every one of us has a part to play in it: private industry, the government.

At the end of the day, someone has to make a decision when there is a problem. But what we really have to do is make sure that we get together and talk about the problems and recognize them. As Dan said, we are all united against an enemy. The enemy may not be the bad guy who is trying to steal credentials. Nation states also represent problems for us. Nation state threats are just as large and just as damaging, if not more damaging. There are some organizations that don't care about the financial impact or

being able to download plans for the Joint Strike Fighter; they want to seek the complete overthrow and maybe the complete destruction of the United States. And that matters as well.

We have to all work together with all of the stakeholders, folks on the technical side, folks on the policy side, people on the business side, to try and be able to recognize the problems, be able to find solutions, fund the solutions and build the solutions. As long as we are doing that, I think on the technical side we are happy. Who runs it doesn't really matter as long as it works. If it doesn't work, I am sure in a couple of years' times, there will be a new leader.

Mr. WEINER. Mr. Nojeim, it does matter, doesn't it?

Mr. NOJEIM. I think it does ultimately, because where the work is located will have an impact on industry participation. And from our perspective, from what we have seen talking to key players in the industry is that one of the things that concerns them is that the program hasn't been transparent enough. If they share information, they don't know how it will be used and where it goes next. So there is this natural tendency to hold back and to think about what happens next.

Where the program is located, where the operations are located impacts on transparency. And so far transparency has been lacking.

From our view, our perspective, it makes sense to have a coordinating body at the White House to do some policy work, to set budgets and do that kind of high-level thinking about this. But operations, they need to be at a lower level, I think. And DHS is a natural place for a lot of this work.

Mr. WEINER. Perhaps. I think there is the concern that this is generally part of a larger conversation about how you foster all that comes from the Internet, good and bad; how you make sure. As I said in my opening remarks, we have resisted the temptation to be heavy-handed plenty of times before. As the Internet emerged, and there were dirty pictures and hateful speech, these other types of things, sometimes we have gotten it right, and I think we got it wrong with gambling. I think to some degree we lurch back and forth, but we have basically defaulted to a position where we have tried to keep our hands off to the greatest extent possible.

I think the vulnerability is that you want to keep hands off, and you don't want to create a situation where you give too much authority to an agency that is used to collecting information and not used to disseminating it, but you want to have a situation where we acknowledge that this does represent a bona fide natural security threat. To whom do you give the authority to do what? Do you give the President the authority to have an on/off switch?

You referred to this in your testimony.

Do you give the President or the NSA or the Commerce Department the authority to go ahead and start experimenting with a second tier of the Internet? These are things that we are going to use to plug in important things like the electric grid or our military secrets or the like.

I think one of the things that you four gentlemen have been helpful in shedding light on is that we really are going to have more

of these headlines. We do need to be cautious. We go through our cycles in American civic life where we see a couple people bitten by sharks, and suddenly there is an explosion of shark bites going on. There have been tens of thousands of attacks that go on. Recently the New York City Police Department said that they get attacked about 70,000 times a day. And we have to make sure that we don't allow the tail to wag the dog here. We want to be thoughtful about it. I think your testimony has been instructive.

Also, I think it is pretty clear, whether it be the Commerce Department or some role for the FCC, we here on the Commerce Committee are committed and frankly have a history of dealing with these issues, looking at not only the security side, but the commerce side and the energy side. If you look at the things that we have talked about today, the Internet itself, interstate commerce, energy issues, commerce issues and the like, I think that this is probably going to be the committee where a lot of these things are going to get discussed even further.

Before I recess, I just want to offer some thanks to people who have helped in addition to those of you who have testified. The record will remain open. If there is anything you would like to submit in written form, any questions and answers you would like to submit for the record, we will certainly be happy to take it.

I just want to thank Tiffany Guarascio of my staff; Amy Levine, Tim Powderly, Roger Sherman and Greg Guice of the committee staff; our friends on the Minority side; and all of my colleagues, as well as the Chairman Mr. Boucher, who has been very active and involved on many of these issues.

I thank you all for your testimony. This adjourns the hearing.
[Whereupon, at 2:41 p.m., the subcommittee was adjourned.]