

CYBER SECURITY: PROTECTING YOUR SMALL BUSINESS

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTHCARE AND TECHNOLOGY

OF THE

COMMITTEE ON SMALL BUSINESS

UNITED STATES

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

HEARING HELD
DECEMBER 1, 2011



Small Business Committee Document Number 112-047
Available via the GPO Website: <http://www.fdsys.gov>

U.S. GOVERNMENT PRINTING OFFICE

72-810

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

HOUSE COMMITTEE ON SMALL BUSINESS

SAM GRAVES, Missouri, *Chairman*
ROSCOE BARTLETT, Maryland
STEVE CHABOT, Ohio
STEVE KING, Iowa
MIKE COFFMAN, Colorado
MICK MULVANEY, South Carolina
SCOTT TIPTON, Colorado
JEFF LANDRY, Louisiana
JAIME HERRERA BEUTLER, Washington
ALLEN WEST, Florida
RENEE ELLMERS, North Carolina
JOE WALSH, Illinois
LOU BARLETTA, Pennsylvania
RICHARD HANNA, New York
NYDIA VELÁZQUEZ, New York, *Ranking Member*
KURT SCHRADER, Oregon
MARK CRITZ, Pennsylvania
JASON ALTMIRE, Pennsylvania
YVETTE CLARKE, New York
JUDY CHU, California
DAVID CICILLINE, Rhode Island
CEDRIC RICHMOND, Louisiana
JANICE HAHN, California
GARY PETERS, Michigan
BILL OWENS, New York
BILL KEATING, Massachusetts

LORI SALLEY, *Staff Director*
PAUL SASS, *Deputy Staff Director*
BARRY PINELES, *General Counsel*
MICHAEL DAY, *Minority Staff Director*

CONTENTS

	Page
OPENING STATEMENTS	
Ellmers, Hon. Renee	1
Richmond, Hon. Cedric	7
WITNESSES	
The Hon. William M. “Mac” Thornberry, U.S. House of Representatives (TX-13), Washington, DC	4
Mr. David Beam, Senior Vice President, North Carolina Electric Membership Corporation, Raleigh, NC	11
Mr. Glenn Strebe, Chief Executive Officer, Air Academy Federal Credit Union Colorado Springs, CO	13
Dr. Phyllis A. Schneck, Chief Technology Officer Public Sector, McAfee, Inc. Reston, VA	15
Mr. Michael Kaiser, Executive Director, National Cyber Security Alliance, Washington, DC	17
APPENDIX	
Prepared Statements:	
The Hon. William M. “Mac” Thornberry, U.S. House of Representatives (TX-13), Washington, DC	27
Mr. David Beam, Senior Vice President, North Carolina Electric Membership Corporation, Raleigh, NC	30
Mr. Glenn Strebe, Chief Executive Officer, Air Academy Federal Credit Union, Colorado Springs, CO	45
Dr. Phyllis A. Schneck, Chief Technology Officer Public Sector, McAfee, Inc. Reston, VA	69
Mr. Michael Kaiser, Executive Director, National Cyber Security Alliance, Washington, DC	79
Questions for the Record:	
None	
Answers for the Record:	
None	
Additional Materials for the Record:	
CompTIA Statement for the Record	93
Recommendations of the House Republican Cybersecurity Task Force	100

CYBER SECURITY: PROTECTING YOUR SMALL BUSINESS

THURSDAY, DECEMBER 1, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON HEALTHCARE AND TECHNOLOGY,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Subcommittee met, pursuant to call, at 1:01 p.m., in Room 2360, Rayburn House Office Building, Hon. Renee Ellmers [chairwoman of the Subcommittee] presiding.

Present: Representatives Ellmers, Tipton, and Richmond.

Also Present: Representative Schilling.

Chairwoman ELLMERS. Good afternoon, everyone. I am going to go ahead and call this meeting to order. I would like to thank everyone for being here joining us today on this very important issue on cyber security. I would like to say a special thank you to Representative Mac Thornberry and our panel of witnesses that will be coming up in the second panel. We appreciate everyone's participation.

Our Nation's digital infrastructure has become an essential part of our everyday lives. It is difficult to imagine a world without the Internet. It touches nearly every sector of the United States economy, and it is critical to our national security. According to the Federal Communications Commission, over 97 percent of small businesses utilize the Internet to increase their productivity and overall success.

On Tuesday, The Wall Street Journal reported that the online sales for Cyber Monday rose to a record \$1.25 billion. This is an increase of 22 percent from last year and marked the heaviest single day for online commerce ever. Despite this good economic news, the growth of the Internet technology and e-commerce has also attracted a growing number of cyber criminals looking to steal sensitive information, including intellectual property and personal financial information. These attacks can be catastrophic, as you can imagine, leaving many businesses unable to recover. Especially our small businesses.

Although we often hear about cyber attacks on large businesses and institutions, a recent report shows the majority of these attacks are on small firms. Small businesses generally have fewer resources available to monitor and combat cyber threats, making them easy targets for expert criminals. Moreover, the sophistication and scope of these attacks continue to grow at a rapid pace.

A recent report from the Office of the National Counterintelligence Executive stated that tens of billions of dollars in trade se-

crets, intellectual property, and technology are being stolen each year by foreign nations like China and Russia. As the leader in producing intellectual property, the United States and small businesses will continue to be a primary target for cyber criminals seeking an economic advantage.

Adding to the uncertainty is the difficulty in which one protects themselves online. Protecting our digital infrastructure is complex, and no one agency or private business can do it alone. It takes a true public-private partnership to identify, combat, and share information regarding these sophisticated cyber attacks.

Both the administration and Congress have recognized the need to update certain laws and resources to better combat cyber threats. The broad range of issues being considered includes establishing a national standard of reporting a cyber breach, strengthening the criminal statutes, and requiring some private industries to develop cyber security plans.

We have heard small businesses' concerns about the possibility of duplicative regulations, always regulations, as many industries already have procedures in place to protect third-party information. For example, a company in my district called Diversified Information Technologies, which digitally processes health care and insurance information, already provides full compliance based on the Health Insurance Portability and Accountability Act, or HIPAA. In considering legislation, we should look to harmonize these regulations to avoid any duplicative rules on small businesses.

There is no question cyber security is a real and major threat to our Nation's economy, security, and everyday way of life. Moving forward, I am confident that we can identify the most efficient role of the public and private sectors to protect small businesses and our Nation against cyber attacks.

Again, I want to thank all of our witnesses who are participating today. I look forward to hearing the testimony on how we can better assist small businesses against cyber attacks. I now yield to the Ranking Member Richmond for his opening statement.

Mr. RICHMOND. Thank you to the chairwoman and thank you to everyone for coming to participate, especially to Congressman Thornberry, who heads the Cyber Security Task Force, and the recommendations that you all have made. So as a person was chair of Judiciary in the State legislature for 4 years, cyber security was under our umbrella, I can tell you that our States are not as aware as they should be of the risk that is posed, so it is a great thing that we are taking the lead on it and that your task force is doing what it is doing. So thank you for that.

Internet and telecommunication technologies have not only changed how we communicate, but also how business is conducted. America's 23 million small businesses are some of the savviest users of technology by using the Internet to access new markets to grow and to diversify. In fact, small businesses are the driving forces behind further technological innovation, as they produce about 13 times more patents per employee. However, along with being connected comes being exposed to new threats. Cyber threats can come in many forms, but they are all devastating to both business owners and to their customers. A single attack can wipe out a small business, which is why cyber crime poses severe problems

for small businesses that are not prepared to mitigate this kind of risk.

According to studies, 40 percent of all threats are focused on firms with less than 500 employees and reveal that a total of nearly \$86 billion annually is lost with companies incurring an average of \$188,000 in losses. Sadly, some small companies fail to recognize the benefit of cyber security as an investment until it is too late.

On the other hand, those firms that understand the importance of such an investment often lack the resources to implement an effective security system. The Federal Communications Commission, the Department of Homeland Security, and the National Institute of Standards and Technology, have all embarked on efforts to offer Federal programs designed to educate the public on computer security. It is worrisome that despite the rise in cyberterrorism over the past few years and the growing impact it has on small businesses, comprehensive cyber security policy remains illusive. With 1.2 million people employed at small companies in the New Orleans metropolitan area, it is important to ensure that they are protected against cyber crimes by keeping our Nation's cyber security, our cyber infrastructure incorruptible. That is why I am cosponsoring the Homeland Security Cyber and Physical Infrastructure Act as a way to strengthen our infrastructure through research, development, and establishment of innovative cyber security technology. Like every day Internet users, small firms are exposed to cyber attacks and vulnerable to their malicious effects.

Today's hearing will give us an opportunity to review whether the increases in Federal investment in both financial and personnel resources will have an impact on a small firm's ability to mitigate their cyber risk. The testimony we hear today will help us better understand what role the government can play in educating the American public and the business community about the security risks and challenges they face. Your recommendations on the best ways to protect the Nation's small businesses from this growing threat will be useful as we move forward on addressing this issue. In advance of the testimony, I want to thank all the witnesses for both their participation and insight into this important topic. Thank you, and I yield back.

Chairwoman ELLMERS. Thank you to the ranking member. I will say that if committee members have an opening statement prepared, I ask that they be submitted for the record. I don't have to explain the timing lights to our first panel of witnesses. It is my pleasure now to introduce, again, Congressman Mac Thornberry, who is our first witness, and he is the Congressman of the 13th District in Texas. He currently serves as the vice chairman of the Armed Services Committee, where he also leads the Subcommittee on Emerging Threats. He continues to serve the House Permanent Select Committee on Intelligence as well.

Earlier this year, Congressman Thornberry was tapped by the Speaker of the House and Majority Leader to spearhead a Cyber Security Task Force to guide House legislation action on this growing economic and national threat. On October 5th, the task force released their recommendations, which have been well received from Republicans and Democrats, the White House, private busi-

nesses and other organizations. Thank you for being here. We look forward to your testimony, Congressman.

**STATEMENT OF THE HON. MAC THORBERRY, A
REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS**

Mr. THORBERRY. Thank you, Madam Chairwoman and ranking member, Mr. Schilling. I appreciate the chance to be here. I have submitted a written testimony, and if it is all right, what I would like to do is just kind of summarize it into four points.

One is, I appreciate you having this hearing. One of the major findings of our task force is that there is a tremendous gap in what is really happening and most people's awareness of what is happening. That is true in the population, it is true among Members of Congress, and our view is that first we have a responsibility to educate ourselves and then try to help our communities understand what a serious issue this is. I have recommended that the Speaker and Minority Leader have a classified briefing for all Members because I think all Members really need to get a better understanding of what we are facing.

Also, just as a test case a few weeks ago, I took a cyber expert with me to my district, and in one town we had a special meeting of the Chamber of Commerce, in another town, it was a joint meeting of the Chamber of Commerce and the biggest service club just to talk about this issue. He could answer the technical questions, but just to try to raise awareness from small businesses in my area, and I hope maybe that is something that other Members may want to consider in the future.

The second point I would make, and both of you have made it in your opening statements, small businesses are affected by this. No one should believe that because I am a small business in Amarillo, Texas, that I don't have to worry about it. It is simply not the case. What we also have come to learn is that not only are small businesses in the cross-hairs of those seeking to perpetrate crime and steal intellectual property, a lot of times small businesses are subcontractors that are used to get to larger contractors. A lot of times increasingly, in fact, lawyers and accountants are targets in order to get their clients' records. So there is some careful planning going on here, but small businesses are particularly in the cross-hairs, and every time they steal intellectual property from a small business, they are stealing jobs from the United States. So it is obviously a national security issue, but as both of you have rightly pointed out, it is also an economic issue that is very important.

Third, I would say that this is a big, complicated issue that Congress cannot solve in a single bill, and we shouldn't try. I think you all have mentioned that it touches most aspects of our lives, most aspects of business life these days. Eighty-five, roughly, percent of the infrastructure we are talking about protecting is owned by the private sector. So government is not going to come in and solve all of this, but we can take steps to help protect the country, and obviously, that is what we need to do.

Fourth and lastly, the task force you have both mentioned have made recommendations as far as a general framework on what Congress could do during this session of Congress, and that was the Speaker's instruction to us, don't try to solve all the problems

in the world, but look at what we can do that will make a significant difference that could get passed during this session of Congress, and our recommendations have drawn on a lot of previous work that Members of both sides of the aisle have done, but I have been pleased at the bipartisan support, not only in the House, but from Senators, the White House has spoken positively of it, so I think there is a real opportunity to act here.

There is lots of differences we have between the parties, between the different Houses of Congress on a variety of issues, but this is one where I think we can work together, and I think it is essential that we work together to try to begin to take those steps in the right direction. So, again, I appreciate your interest in it, and I will be happy to answer any questions that I can answer.

Chairwoman ELLMERS. Well, I definitely echo those comments about the importance of us all working together in a bipartisan manner on this issue, I think we all see the very important aspects of it.

I just have a couple questions, and then I will yield to Mr. Richmond, the ranking member. My first question for you, Congressman, is the recent report from the National Counterintelligence Executive Agency revealed that China and Russia are behind a majority of cyber attacks, and that is obviously deeply, deeply disturbing. In your opinion, how does the small business, the small business that is out there right now dealing with all of the issues with the economy, how can these small businesses deal with these attacks right now, and what and how should the United States respond to this as a Nation?

Mr. THORNBERRY. I would say two things, and they are really the central recommendations of our task force. Number one is what is called good hygiene. It is the basic things that we all know we should do but too often don't do, keeping our firewalls up to date, our virus protection up to date, not having our passwords underneath our mouse pads in our offices, which a defense contractor told me he just went and checked in one of his offices and found that was the case in a large number of his employees, and the task force received information from a variety of witnesses saying roughly three-fourths of the malicious stuff out there on the Internet could be stopped if we all did the basic stuff we know we are supposed to do. You know the reason they call it good hygiene because it is kind of like washing your hands and coughing in your sleeve and getting enough sleep and drinking enough water, the basic things that keep us healthy, it can keep the Internet healthy, too. So small businesses, you know, it doesn't take a lot of money, but you need to do the stuff you know you should do.

Secondly, though, when you talk about Russia and China, if Russia and China is targeting somebody, good hygiene won't be enough, and so our second central recommendation is to update some laws to allow information sharing that where we can use especially Internet service providers to help defend us against these more sophisticated threats. And so I think you have got to do two prongs: Basic hygiene, but also update our laws so that we can bring all the resources of government and the private sector to bear against these more sophisticated threats.

Chairwoman Ellmers. Thank you. My next question for you, there again, comes from our small business owners, and they are basically saying that, you know, one of the big issues, and we hear this repeatedly, is the threat of regulations and dual regulations, especially those industries defined as critical infrastructure. This is a two-part question here. First, has this issue been adequately addressed, and in your opinion, do you believe that small businesses should be subjected to the same regulations or Federal standards as larger businesses regarding cyber security compliance?

Mr. THORNBERRY. It certainly has not been adequately addressed, and I think this gets to where there is a difference of opinion between the White House proposal that came out in May and the task force recommendation. The White House recommended basically that critical infrastructure businesses develop a cyber security plan which would be sent to the Department of Homeland Security for evaluation and kind of a thumbs up or thumbs down. Our view was that we ought to rely on existing regulators, so for the electric industry, FERC, and NERC and the existing regulators, the Nuclear Power Regulatory Commission for nuclear power plants, et cetera. In other words, these structures are in place, they help understand the fuller spectrum of what these businesses are dealing with, and they need to put a greater emphasis on cyber security.

Now, we are going to have to work through how to do that, but I think I am concerned, as you mentioned, about layering additional regulations, particularly on small businesses that have a difficult time affording what they have got now.

Chairwoman ELLMERS. Thank you. Thank you for outlining that. There again, you know, having to report to more than one agency, each of these different duplicative just adds to the cost of doing business as well, so—

My last question, in actually talking about Federal agencies, of course, Federal agencies play a key role in protecting against cyber attacks. Considering our committee, Small Business Committee and its jurisdiction, what do you think the appropriate role is for the Small Business Administration?

Mr. THORNBERRY. My sense is the most valuable thing is the awareness and help small businesses have the tools to know how to defend themselves, and if you can do that where you don't have to go hiring an outside consultant or so forth, if you can just help direct small business to the kinds of things they need to do with that good hygiene we were talking about, I think that would be a tremendous help to small business, but again, when you help all those small businesses, you are also helping the whole Internet because you reduce the clutter that is out there, and that helps the more sophisticated entities target those more sophisticated threats.

Chairwoman ELLMERS. Thank you so much for answering my questions. I am going to yield now to Mr. Richmond for his questions.

Mr. RICHMOND. Thank you, and I will try to start where you are leaving off when we talk about education and awareness as a cost-effective way to reduce our cyber breaches. The task force suggested the basic technology tools, industry best practices, and education could eliminate about 85 percent of the cyber threat. I think

you just hit on most of it, but what else besides the good hygiene and the other recommendations can we do to further push for a reduction and further accomplish a reduction in cyber attacks?

Mr. THORNBERRY. Well, one of the key areas, we believe, is that we need to provide some voluntary incentives so that as a CEO is trying to figure out where his money goes, that more of his attention and perhaps more of his money goes to defending that business against cyber attack.

Now, again, there are some differences. There are some people who have made proposals on a more directive regulatory approach. Our view was you can't have one size that fits all, but a variety of incentives, whether it is the Tax Code, whether it is SEC regulations, which actually they came out with one a couple weeks ago that requires greater attention be paid to cyber.

I think that sort of thing, we have got to elevate this issue in the consciousness not only of Members of Congress, the American people, but of businesses, and some incentives, financial incentives, I think—we think help accomplish that, even though we did not try to put out a laundry list of what they all are, and suggestions that you all may have, particularly for incentives that would be effective for small business, I think, would be very welcome as we move through this process.

Mr. RICHMOND. Another thing, one of the recommendations was in the Federal procurement process, to require security technology processes and performance management in the government IT process. Since we are sitting on Small Business, one concern that immediately pops up is the cost associated with it and how would it put small businesses at a disadvantage compared to other businesses in the procurement process for government contracts.

Mr. THORNBERRY. It is a good point. I think our view was, the government is a big customer, we ought to be a good big customer in what we buy, in other words buy things that are more secure, but also I think what one finds out is a lot of innovation in this area is being done by small business, innovation in enhanced security. So I think, if we can put a higher priority on security that small business, particularly small business innovators will benefit from that. They should, and I hope so.

Mr. RICHMOND. I am glad you brought up the role that small businesses play in the technology aspect of it. The Federal Government is spending an enormous amount of money, and we are spending more every year, on cyber security. What niche, or what way do you see small businesses being able to participate on the technology side of helping us get ready, combat or fight off cyber attacks?

Mr. THORNBERRY. I think we were just touching on it. A lot of the innovation that goes on is in small business start-up businesses, and the Federal Government in its procurement has to be nimble enough to take advantage of those advances, and that is obviously a challenge. And a second area that we touched on is, the Federal Government spends a lot of money on research in cyber. We ought to make sure the money we spend on research in cyber is not taking the place of money that private industry is spending on cyber. In other words, displacing some small business that is putting their resources out there, we ought to be complementary,

more basic research that everybody can benefit from rather than researching things that, you know, that put a small business potentially out of business.

Mr. RICHMOND. And just a few more. When you talked about information sharing earlier, of course it raises questions of privacy concerns. One question that would quickly pop up in my mind is in an information sharing arrangement, for the person whose information is then leaked or who has his life or business turned upside down because of it, how do we address liability in that question and who ultimately would bear the responsibility?

Mr. THORBERRY. It is, in many ways, kind of a central question to making this work, you are exactly right. What we recommended in the task force was creating a separate entity apart from government where information could be shared so that—and I will just take the car industry. For example, Ford and GM could bring their information to this place to share. They may want to sanitize that information so you don't have particular individuals' names and so forth, but they could bring the information that we are getting attacked from here, we are getting attacked from there, threat information could come together.

At the same place you would have government classified information brought in so that you can have this whole fuller picture, at least, of the nature of the threat with appropriate classified safeguards so that we do not lose important national security information, and then ideally, that information could be acted upon by Internet service providers, so you accumulate this threat information, and AT&T and Verizon can use that information to protect big businesses and small businesses eventually, hopefully.

I mean, that is kind of the concept that we talked about, but you are absolutely right that privacy has got to be built in every step of the way and that if we don't, the American people are not going to go for it, and we will not be able to advance cyber security.

Mr. RICHMOND. And the last question is hopefully a short answer, but nowadays with iPads, iPhones, Androids, so between the smartphone and the tablet, they are becoming business instruments for many people, especially small businesses. What is your assessment of what cell phone companies and those companies are doing in terms of making sure that there are adequate safeguards in place for threats on those smart devices?

Mr. THORBERRY. As they multiply, the potential entry points for attacks of some sort multiply as well, and I don't think there has been nearly enough attention by the software companies, the hardware companies or us as individuals into safeguarding these little devices that we all carry around with us.

But I will say, from the Armed Services Committee standpoint, we are going to start issuing some of these devices to soldiers in the field, and so we have got to figure out from a government standpoint how we make sure they are secure, and hopefully that can start a trend towards greater security for all of these devices.

Mr. RICHMOND. And I am glad you mentioned that, and this will be the last question.

Chairwoman ELLMERS. That is fine.

Mr. RICHMOND. What you just said scares me because I think of my smartphone and the fact that it has great capabilities where

parents can use the GPS feature on their children's smartphone to see where they are, the first question in my mind becomes whether the technology is there, whether the companies have the ability to make sure that we are not giving away the coordinates and where our soldiers are, but, you know, so do you think that—and I know that our military and our leaders would address those things, but those types of concerns, we just have to make sure that those cell phone providers and those are very wary of those, especially as more and more—and we talked about troops, but especially as more and more children have cell phones, we have to worry about the cyber attacks. We also have to worry about our hardened criminals using technology to find our children and so forth.

So that is one thing we have to keep pushing on our industries and our companies, to make sure that they understand to some extent there is a moral responsibility with making sure that the phones are as safe as possible in that respect. So thank you for what you do, Mac, and thank you to the Chairwoman for allowing me a little extra time. Thank you.

Chairwoman ELLMERS. Well, thank you. Those were excellent questions, excellent questions, and excellent responses. This is quite an opportunity today.

At this time, I would like to recognize Mr. Schilling from Illinois, if he has any questions.

Mr. SCHILLING. Yes, thank you, Chairwoman. I think I agree with Mac here, with Congressman Thornberry I should call him, is this is something that really needs to be addressed, and, you know, as I go into some of the hearings that we have been in, some of the briefings, you know, I don't really feel a sense of urgency out here in Washington, D.C. when it comes to the cyber attacks that we are already dealing with, and then the future ones that are coming, and being a small business owner myself, you know, of course, one of the things that I always fear is when I hear the government is going to get into and then they are going to throw something else upon my small business that is already struggling, things like that, so I think that is something we definitely need to work on.

One of the things I was curious is, where is, like, leadership, for example, on maybe having briefings with the Democrats and Republicans here to where we can get the message? And I really appreciate, just the idea that you had of going out to the Chambers and speaking to the small businesses because this is a real threat, and I think down the road, this is going to be something that we are going to have to really pay a lot of attention to. So several different—

Mr. THORNBERRY. I think there is a good chance it will happen. As I mentioned, I recommended to the Speaker, I know Jim Langevin talked to Mrs. Pelosi's office about jointly doing this. Obviously, I think you are right, generally there is not the sense of urgency. For people like the Speaker, the President, and the Majority Leader in the Senate who have had every day or every week get classified briefings, they are pretty fired up about this, and see the urgency of doing something. So I am hopeful we can do that, and I think it would help all Members to get a little fuller picture of what we face every day.

Mr. SCHILLING. Very good. I do like the message you have, also when we do do something, is it something that is going to complement somebody that is already working on something, not trying to take something that maybe a small business is working on. So that is all I had. Thank you.

Chairwoman ELLMERS. Great. Thank you. At this time I would like to recognize Mr. Tipton from Colorado.

Mr. TIPTON. Thank you, Chairwoman, and Congressman, thanks for your leadership on this obviously very important issue. I haven't had an opportunity to obviously be able to go through your entire task force report, but in there, it states that 85 percent of the issues, cyber issues can be cleaned up with hygiene, and I was wondering, is there a way to be able to really accomplish this without driving up some of the costs that small businesses are really going to be bearing? Any estimates on that?

Mr. THORNBERRY. Well, I think you can do it with incentives and encouragement. Maybe you don't get all 85 percent. Maybe you get 80 percent. But I think increasingly, small businesses, like all businesses, are going to have to understand that if their customer records are stolen and misused, they may have some responsibility for that, and so I think we are better off in structuring things where it is self-interest to put a higher priority rather than government mandating how it should be done. Among other things, the threats move so quickly, there is no way the government can regulate in this area. It just evolves so fast. But as in some other areas, physical safety, for example, everybody has to have insurance, sometimes you have an insurance agent come and inspect your physical plant to determine your rates and so forth. That is the sort of incentive, I hope, that we can get going.

Mr. TIPTON. Great. And I apologize for being late, and if you have already answered this, but I was also curious where you had noted that a number of our small businesses are developing new technologies that are being hacked and the next day they know it is out on to the street, are there any estimates in terms of how much that is costing the U.S. economy?

Mr. THORNBERRY. I don't know of any good estimates. You have a wide range of numbers about the value of the information being stolen every day, every year from our economy, but we did hear specific instances of small businesses who discovered that they were hacked and information, where there was a formula, a blueprint, something was taken from their computers, and a few months later that exact product shows up on our shores with "Made in China" stamped on the back. Now the problem is they knew they were hacked. How many are out there that don't know that the information was ever stolen from them. So that is part of the reason we believe we have got to make this a bigger deal for everybody.

Mr. TIPTON. Exactly. Again, thank you for your leadership. Madam Chairman, yield back.

Chairwoman ELLMERS. Thank you. Again, I would like to thank Congressman Thornberry for his leadership and insight on this issue. We will continue to work closely with his office and the task force on developing legislation that assists small businesses in combating cyber security. Thank you so much. It was a pleasure.

I would like to call the second panel now to the table.

Wonderful, let's go ahead and get started. I would like to take the opportunity right now to just explain to you the timing lights. You will each have 5 minutes to deliver your testimony. The light will start out as green. When you have 1 minute remaining, the light will turn yellow. Finally, it will turn red at the end of your 5 minutes, and I ask that you try to keep to that limit, if possible, although, you know, I am usually pretty flexible with that within reason. Within reason.

Thank you all for being here. Again, this is a great opportunity. It was certainly wonderful to hear from Congressman Thornberry. He has done so much work on this, and now from the business aspect, you know, we get to hear your side of it. So, again, thank you so much for being here today.

I am going to take the opportunity now to introduce our first witness, Mr. David Beam. Before I do, though, I do want to say that at some point we may be called for votes, and what we will do at that time is we will interrupt, we will kind of decide what time frame we are looking at, and then we will come back and pick up again later, okay?

So our first witness is Mr. David Beam. He is the senior vice president of Corporate Strategies for the North Carolina Electric Membership Corporation in Raleigh, North Carolina. David has over 30 years of experience in the electric utility industry. In his current role, he oversees their energy risk management and regulatory compliance, including cyber security. David earned his Bachelor of Science in mechanical engineering from the University of Kentucky and his MBA from the University of North Carolina Chapel Hill. He is testifying on behalf of the National Rural Electric Cooperative Association.

STATEMENTS OF DAVID BEAM, SENIOR VICE PRESIDENT, NORTH CAROLINA ELECTRIC MEMBERSHIP CORPORATION, ON BEHALF OF THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION; GLENN STREBE, CHIEF EXECUTIVE OFFICER, AIR ACADEMY FEDERAL CREDIT UNION, ON BEHALF OF THE NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS; PHYLLIS SCHNECK, CHIEF TECHNOLOGY OFFICER PUBLIC SECTOR, MCAFEE, INC, ON BEHALF OF THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION; AND MICHAEL KAISER, EXECUTIVE DIRECTOR, NATIONAL CYBER SECURITY ALLIANCE

Chairwoman ELLMERS. Welcome, you have 5 minutes to present your testimony.

STATEMENT OF DAVID BEAM

Mr. BEAM. Chairman Ellmers, and Ranking Member Richmond, thank you for inviting me to testify on cyber security impacts on small businesses. My name is David Beam, and I am senior vice president of Corporate Strategy for North Carolina Electric Membership Corporation, or NCEMC. NCEMC is a generation and transmission cooperative providing wholesale power and other related services to 25 of the 26 electric cooperatives incorporated in North Carolina. NCEMC is responsible for reliability in cyber secu-

rity compliance, for its own critical assets as well as those belonging to its members. These assets include generation and transmission facilities and the associated protection equipment and procedures. All of our distribution cooperatives that own NCEMC are small businesses. I would like to acknowledge the National Rural Electric Cooperative Association. NRECA is our national trade association representing over 900 cooperatives nationwide, providing electricity to 42 million consumers in 47 States.

Today I will cover the following: The bulk power system and how it is separate from the distribution system, the origin and purposes of the North American Electric Reliability Corporation, or NERC, how we comply with NERC reliability and cyber security standards, and our views on the potential impacts of new legislation. I would also like to commend the work of Speaker Boehner's Cyber Security Task Force and the leadership of Representative Mac Thornberry.

Generally speaking, NERC's standards apply to the bulk power system which includes generation and transmission assets operated at voltages of 100 KV or higher. Distribution facilities receive power from the bulk power system and transmit it to retail consumers. Because outages at the distribution level generally do not pose a threat to the bulk power system, NERC standards don't typically apply to distribution lines and substations. Contrary to popular belief, hackers cannot easily access the telecommunications systems that overlay parts of the bulk power system. Utilities have comprehensive cyber security systems to protect against malicious attacks.

Congress created a mandatory enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005. NERC is an industry-funded, self-regulatory organization. Its purpose is to regulate reliability and cyber security standards. It also audits compliance and has enforcement authority over those standards. NERC and the Federal Energy Regulatory Commission or FERC can fine utilities that violate these standards and have done so. Additionally, FERC can direct NERC to develop new or revised reliability standards.

Congress created a stakeholder-driven process, recognizing that utility owners and operators best know how to provide reliable electric service and how our complex systems are designed and operated. We want to preserve this process.

NCEMC follows exacting procedures to ensure NERC compliance. Our goals are awareness and commitment to compliance by all employees, prompt detection, cessation, and reporting of violations, and effective remediation measures should violations occur. NCEMC has devoted significant financial and human resources to ensuring reliability in cyber security. We employ a full-time compliance coordinator whose sole responsibility is managing compliance with reliability and cyber security standards. In addition, NCEMC employs a compliance team of subject matter experts who are responsible for compliance with their assigned cyber security and reliability standards. NCEMC also uses outside contractors to audit and provide recommendations for improving our compliance program. Additionally, at least one employee for each distribution co-

operative is responsible for compliance with reliability and cyber security standards.

We employ strong defensive measures to protect our network and business systems. We have strict security guidelines for securing the network and systems, including policies that govern the access and use of its network and systems. NCEMC and NRECA believe NERC processes work very well. The process could be strengthened by narrowly targeted legislation that lets the Federal Government react quickly to severe, imminent cyber threats and increases timely actionable information flowing to utilities. Any new legislation should cover only assets and systems which are realistic targets of cyber threat and which could truly impact the bulk power system. Casting too wide a net could bring entities, like distribution co-ops and other small businesses, under potentially very burdensome regulatory requirements with little or no benefit to grid security.

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

Chairwoman ELLMERS. Thank you, Mr. Beam.

Chairwoman ELLMERS. I now yield to Congressman Tipton for the introduction of our next witness.

Mr. TIPTON. Thank you, Chairwoman. It is my pleasure today to be able to introduce Mr. Glenn Strebe. He is the chief executive officer of the Air Academy Federal Credit Union in Colorado Springs. He oversees full operations of nine credit unions, including oversight of their compliance and security issues. Glenn received his Bachelor of Science from the U.S. Air Force Academy, my son-in-law is also a graduate of the Academy, and an MBA from the Colorado State University. He is testifying on behalf of the National Association of Federal Credit Unions, and Glenn, welcome, and we look forward to your testimony.

STATEMENT OF GLENN STREBE

Mr. STREBE. Thank you. Good afternoon. Chairwoman Ellmers, Ranking Member Richmond, and members of the subcommittee, my name is Glenn Strebe, and I am testifying today on behalf of the National Association of Federal Credit Unions, or NAFCU. Thank you for holding this important hearing. I appreciate the opportunity to share my views on cyber security and data security at our Nation's credit unions. NAFCU supports efforts to enact comprehensive data and cyber security measures to protect consumer data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act. Unfortunately, there is no comprehensive regulatory structure similar to what was put in place for financial institutions under Gramm-Leach-Bliley for other entities that may handle sensitive personal and financial information. Consistent with Gramm-Leach-Bliley, the National Credit Union Administration established administrative, technical, and physical safeguards for credit unions to ensure the security, confidentiality, integrity, and proper disposal of consumer information and other records. Every credit union must develop and maintain an information security program to protect data. Additionally, the rules require third-party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of this information.

Gramm-Leach-Bliley and its implementing regulations have successfully limited data breaches among financial institutions. I have outlined the specifics of the Act in my written testimony.

At Air Academy Federal Credit Union, we are relentless in our efforts to protect sensitive data. The increased reliance on Internet-based services has created new challenges and expenses over the past decade. With over a quarter of our members living out of State, a large number of our transactions are performed online. In order to address this growing trend, Air Academy has implemented and continues to execute security measures on many different levels, the details and costs of which are outlined in my written testimony. At Air Academy, we take cyber security seriously. We use an ethical hacker that tests our security measures, looking for hidden vulnerabilities. Our laptops and thumb drives are encrypted in case they fall into the wrong hands. We change penetration testing vendors as well as our service providers every 2 or 3 years to avoid complacency and to keep a fresh set of eyes on our security system. While all of these steps are costly, they are best practices. Despite Air Academy's efforts, the inadequate security systems of other entities still leaves our members' data vulnerable to hackers and thieves.

Everyone has heard about large national data breaches that impact millions of payment cards, but many breaches are small and on the local level. For example, in 2009, a local liquor store failed to protect card data because they claimed no liability. We suffered over \$60,000 in losses. Data breaches are a serious problem for consumers and businesses.

Financial institutions such as credit unions bear a significant burden as they incur steep losses in order to reestablish member confidence after a data breach occurs. NAFCU has developed a list of items we would like to see addressed in any data security bill. They are outlined in detail in my testimony and include: Payment of breach costs by breached entities; national standards for safe-keeping of information; disclosing of data security policy at point of sale; requiring disclosure of the breached entity; enforcement of prohibitions on data retention; and timely notification of account servicer when a breach occurs.

In conclusion, NAFCU supports new measures to protect consumers' financial data. Creating a comprehensive regulatory scheme for those entities that currently have none is critical. A safe harbor for financial institutions already in compliance with Gramm-Leach-Bliley should be included in any data security bill. Further, if more regulations are needed to address new concerns, it should be the functional regulators that are charged with promulgating new rules. Finally, any other party that holds sensitive information should be held liable when responsible for a data breach.

Thank you again for the invitation to testify before you today. I would welcome any questions you may have.

Chairwoman ELLMERS. Thank you, Mr. Strebe.

Chairwoman ELLMERS. I now yield to Ranking Member Richmond for the introduction of our next witness.

Mr. RICHMOND. Thank you, Madam Chairwoman. It is my pleasure and honor to introduce to everyone Dr. Phyllis Schneck, who

is the chief technology officer for the public sector at McAfee, a leading provider of cyber security software. Ms. Schneck received her Ph.D. in computer science from Georgia Institute of Technology where she pioneered the field of information security and security-based high performance computing. In addition to her role at McAfee, she currently serves as the chairman of the board of directors of the National Cyber Forensics and Training Alliance. Ms. Schneck was named one of the top 25 women leaders in information security, and she also holds three patents in high performance and adaptive information security. Welcome, Ms. Schneck. I am sorry, Dr. Schneck.

STATEMENT OF PHYLLIS A. SCHNECK

Ms. SCHNECK. Thank you. Good afternoon, Chairwoman Ellmers, Ranking Member Richmond, and members of the subcommittee. I am Phyllis Schneck, vice president and chief technology officer for the global public sector for McAfee, testifying today on behalf of the Software & Information Industry Association. SIIA is the primary trade association of the software and digital information industry, with more than 500 members that develop software and electronic content for consumers, business, education, and the Internet. McAfee, Inc., protects businesses, consumers, and the public sector from cyber attacks, viruses, and a wide range of cyber security threats. We are the world's largest dedicated cyber security technology company and a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of the Intel Corporation.

We appreciate the subcommittee's interest in cyber security as it affects small business, which plays such a large part in our Nation's economy. While small business falls prey to the same security risks as large business, most small firms cannot afford a dedicated security staff nor do they have a million dollar budget to purchase enterprise security solutions. Nevertheless, small companies must meet the same security and compliance requirements as Fortune 500 firms, just to remain in business.

The importance of small business to the national economy cannot be overstated. According to the Small Business Administration, small firms represent 99.7 percent of all employer firms. They have generated 65 percent of new jobs over the past 17 years, and as Ranking Member Richmond mentioned earlier, they produce in order of magnitude more patents per employee than even the large patenting firms.

Today's cyber threats are more sophisticated and targeted than ever. They are growing at an unprecedented rate. McAfee Labs finds, for example, that both malicious URLs and malware, they have grown almost sixfold in the past 2 years, and in 2010 we saw more malware than in all of the years previously.

One of the most insidious cyber attacks is a low level incursion, it sinks below the radar, quietly exploring and stealing the contents of the network. Security professionals call this an advanced persistent threat on an APT, and McAfee has uncovered several over the past year, the most recent, shady RAT, has been stealing valuable intellectual property from more than 70 organizations across 14 countries, including small firms in addition to govern-

ment contractors, nonprofits, and government agencies. And this is not an isolated incident. A 2010 survey found that 60 percent of organizations report a chronic and recurring loss of sensitive information.

More than a million small businesses and retailers were victims of some type of information theft in 2010, with 56 percent of small and midsized businesses experiencing this type of banking related fraud in 2010 and 75 percent of it coming from online sources. Among small businesses falling prey to bank fraud, 61 percent were victimized more than once.

We are only as secure as our weakest link. To further help small business, we recommend three guiding principles to make the cost of security most effective. Practice risk management first. Next, minimize the amount of sensitive information retained in the network; and, third, invest in the appropriate level of security.

Finally, we have some policy recommendations. A heavily regulated approach would not necessarily make organizations more secure. It makes them more compliant. And it would stifle innovation. On the other hand, positive incentives and subsidies have a high probability of success in two ways: First, a higher chance of better actual outcome; and secondly, a higher probability of good legislative success. There are a variety of proposed approaches found on incentives, including the recommendations that we heard earlier from Representative Thornberry of the House Republican Cyber Security Task Force and some promising approaches on the Democratic side.

We support the following approaches:

Litigation and legal reform. Imposing limitations on liability for damages as well as for noneconomic loss would remove a serious obstacle to information security investment, such as the risk of being held responsible for losses notwithstanding a company's good faith investment in good cyber security.

Public-private partnership on information sharing. Departments of Defense and Homeland Security manage many public-private partnerships, McAfee plays a key role in several. These partnerships ensure that senior corporate and government officials share vital information and best practices, and they are especially important for small businesses.

Competition, scholarships, research and development help identify and recruit talented individuals that foster innovation in advanced basic and applied solutions and bring those individuals to the cyber security workforce.

Tax incentives. Accelerated depreciation or refundable tax credits should be considered to encourage critical infrastructure industries to make additional investments in cyber security technologies, solutions, and human capital. The same approach could be effectively applied to small business.

Insurance reforms. Because of the lack of actuarial data, government should consider implementing reinsurance programs to help underwrite the development of cyber security insurance programs, which could be phased out as insurance markets gain the cyber security coverage.

In conclusion, let me emphasize that collaboration and cooperation between the public and private sector are key to addressing

cyber security in a holistic way. Thank you for your interest, and I will be pleased to answer any questions.

Chairwoman ELLMERS. Thank you, Dr. Schneck.

Chairwoman ELLMERS. I have the opportunity now to introduce our last witness for today, Mr. Michael Kaiser. He is the executive director of the National Cyber Security Alliance, NCSA, in Washington, D.C. The NCSA is a nonprofit organization focused on educating and promoting awareness of safe cyber security practices to individuals, education institutions, and small businesses. They recently conducted a study analyzing small business cyber security practices. Welcome, Mr. Kaiser. You have 5 minutes for your testimony.

STATEMENT OF MICHAEL KAISER

Mr. KAISER. Thank you, Chairwoman Ellmers and Ranking Member Richmond, and members of the subcommittee. Thank you for the opportunity to testify today on this very important current state of cyber security in small business. My name is Michael Kaiser, and I am the executive director of the National Cyber Security Alliance. NCSA is a nonprofit organization, a public-private partnership working with industry leaders, government, and nonprofits on education awareness issues in cyber security. NCSA's board of directors is comprised of representatives from 18 companies, ADP, AT&T, Bank of America, Cisco, EMC, ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin, McAfee, Microsoft, PayPal, SAIC, Symantec, Verizon and Visa.

NCSA leads cyber security education and awareness in this country. We lead critical efforts, such as the STOP. THINK. CONNECT. campaign, which we developed with the Anti-phishing Working Group and industry and government and which the Department of Homeland Security leads in the Federal Government. We have developed National Cyber Security Awareness Month, we are working on Data Privacy Day, and we operate StaySafeOnline.org, our Web site. NCSA recently signed an MOU with the Department of Education and NIST to lead the National Cyber Security Education Council, a public-private partnership to address formal cyber security education from basic education all the way through to degrees and workforce training programs. We have a long track record in conducting surveys about the practices of individual small businesses and the state of cyber security in U.S. schools.

In October, we released the results of a study conducted in conjunction with Symantec about the cyber security practices of small businesses. We found that businesses still don't have good practices and policies in place, allow risky behavior, and in general, fail to take a strategic approach to cyber security, leading unfortunately to a false sense of security. We found actually that businesses are becoming more reliant on the Internet. Two-thirds say that their business is dependent on the Internet for day-to-day operations and also two-thirds say they have become more dependent on the Internet in the last 12 months. A majority, 57 percent, say that the loss of the Internet access for 48 straight hours during a regular business week would be disruptive to their business.

We learned that businesses actually have critical information on hand. Sixty-nine percent report handling customer data, half deal in financial records and reports, one-quarter have their own intellectual property, which we have been discussing a lot today, and actually one-fifth have the intellectual property of other people in their business, which I think is something we have to be concerned about as well.

We discovered that small businesses aren't creating an environment that promotes cyber security. Seventy-seven percent do not have formal Internet security policies for employees, and nearly half of those don't even have informal cyber security policies for their employees. Sixty-three percent don't have policies that relate to the use of social networks in the workplace, and two-thirds allow the use of USB devices in the workplace. These are general risk factors that we are aware of.

Unfortunately, these data show that the entire small business ecosystem is at risk, and we look at it that way a lot. We need to reach every small business with information that will help them protect their digital assets. Cyber criminals, as has been mentioned here, are well aware of these vulnerabilities, and small businesses have become a primary target for them. 40 percent of all targeted attacks are directed to businesses with less than 500 employees, and roughly 60 percent close within 6 months of a cyber attack. It is tough enough for small businesses to make and thrive, we shouldn't also be losing them to cyber criminals. There is no single government agency, nonprofit group that can take on—company, government agency or nonprofit group that can take on this vast issue alone or reach every small business. Working together with a broad array of stakeholders, leveraging resources, sharing the responsibility is our best hope for success.

Based on this thought of a collaborative approach, here are some ideas that we have about what we could do. Create a harmonized message in a campaign, like STOP. THINK. CONNECT. that can be deployed by key stakeholders. That would go a long way to clarifying for business owners what they need to do, and it would come from trusted sources.

Align forces within the Federal Government to support small businesses. Many Federal agencies have an interest in helping small businesses grow and protect their digital assets. At minimum, the Small Business Administration, the Department of Commerce, the FTC, the FCC, the Department of Homeland Security should participate, but others such as the Department of Defense and the IRS that work and touch small businesses should be involved as well.

Engage local communities in the effort. Small business owners are likely to listen to their local peers. A few forward-thinking communities, such as Washtenaw County, Michigan, San Diego, California, San Antonio, Texas, and Colorado Springs have started efforts to make their communities more cyber secure, and they have all prioritized small business as a key target in their communities to make that happen.

Support education reform that leads to a more cyber capable workforce. We need a workforce in the 21st century that under-

stands how to use technology safely, securely, ethically, and productively when they graduate high school or college.

And encourage your colleagues, I think as Representative Thornberry has done, to make information available to small businesses in your district. Go out, talk with them, have a town hall on cyber security, and get the conversation going.

Thank you for your time and attention to this issue, and I look forward to your questions.

Chairwoman ELLMERS. Thank you, Mr. Kaiser. We are going to go ahead and get started with some questions, and just so you know, we will be called for votes about 2:15, so what I am going to do is I am going to yield now to Mr. Tipton from Colorado for his questions.

Mr. TIPTON. Thank you, Madam Chair. Glenn, I would like to thank you for joining us. Once again, it is good to have a Coloradoan here and to be able to see you. I was disturbed a little bit, the stories that you had in your written testimony about the costs to your businesses in terms of the data breach from the other company, I believe it was a liquor company; is that right?

Mr. STREBE. Yes, it was.

Mr. TIPTON. The mistake ended up costing you thousands of dollars for nothing you had no control over, and you also mentioned that you were only able to recover 35 percent of your incurred expenses. What additional steps would you recommend that Congress and this committee take to curb this phenomenon and without imposing burdensome regulations on small businesses?

Mr. STREBE. As I mentioned in my verbal comments as well as in the written testimony, one of the things that does not occur out in the business world is the fact that there is no liability, there is no accountability. In the case of that liquor store, the police were involved in that case, and they themselves were confronting the liquor store, asking them, you know, What are you doing? They said, Well, we don't have any liability, so we are really not going to worry about it, and as a result of that it cost us over \$60,000. What would I do? I would look for the opportunity to hold accountable, as I have written in testimony, hold accountable those businesses that have such a cavalier attitude.

Mr. TIPTON. I appreciate that. And Dr. Schneck, I believe in your comments you said that we have got to be very cautious that we just aren't in a manner of compliance as opposed to having the security. Would you like to expand on that a little bit because I think as small business people we often see, we spend a lot of time making sure we are complying as opposed to getting the job done.

Ms. SCHNECK. Thank you. The problem with regulation is that it draws a box, it draws a box where they have to take the money and invest, and it does two things: Number one, it stifles innovation because if companies are only having to fill that box and invest in those X places, it doesn't leave a lot of room for advancing creativity, saying well, how else can we solve this problem that might be better because the regulation is this is what we have to buy, it is in this box.

The second thing it does that can really hurt small businesses, it shows the adversary, the cyber adversary, everything that is outside of the box, and small business is already a target, as has been

mentioned, not only a target to bounce into a larger enterprise, but small businesses, in many cases, are developing the intellectual property that could make the next jet engine and working on national security and holding private information, all kinds of ways.

So they are holding the same intellectual property and harboring the same risk as a big company that can afford a dedicated team and the best security, but they can't afford, they don't have the extra money to do that to secure their piece, and at the same time what regulation would do is show the outline of the box and show the bad guy exactly where he can go straight into those small businesses that can't afford to protect it, so what we really need to do is incentivize, and as was mentioned by Representative Thornberry and some other colleagues, some good incentives for businesses to be able to target that investment upfront, make cyber security part of the corporate risk and go ahead, as I mentioned, and minimize the amount of information that is stored on their network. Compliance and regulation are not going to protect us.

Mr. TIPTON. So be very cautious about trying to have a one-size-fits-all regulatory policy?

Ms. SCHNECK. Exactly. Or anything that doesn't allow innovation.

Mr. TIPTON. Thank you so much. I yield back, Madam Chair.

Chairwoman ELLMERS. Thank you. I am going to go ahead and ask my questions now. This question I would like to ask the entire panel for your opinion. There is a variety of Federal agencies and organizations involved in combating cyber security, as you know. Do you think small businesses know where to go to get the best information and assistance and, if not, what recommendations do you have to help us get that information out? Starting with Mr. Kaiser.

Mr. KAISER. Yeah, you know, we take approach to all this, a similar approach across all education and awareness in cyber security on this issue, which is that we should not try to spend a lot of time trying to get, in this case, small businesses to trust other entities for new information. We should be going to the entities that they already trust and getting them to disseminate a very similar comprehensive harmonized message, so whether it is in their vertical of their industry or to a government agency that they already trust or back to a software provider on an ISP, if we can coordinate and harmonize that messaging, then they will just go to who they trust, and no matter where they go they will get the right message. I think that is really the work that we have to do at this level to support them at the lower levels.

Ms. SCHNECK. I would definitely agree and echo those remarks. I would add that the cyber adversary is fast, shares information very well, already has trust, is often very well funded. So they can act without any legal boundaries, IP boundaries, and that is why they are winning. The very best thing that we can do as the good guys is match that and then go one step better. Since small business makes up 99.7 percent, I calculate that as part of the fabric, they are a large part of the cyber information and situational awareness that we will see, breaches, how they happen, what they are seeing. First and foremost, we would ask them to know who to call, whether it is a partnership of law enforcement or others that

you trust, know who that is ahead of time so that you can all get together when you see something, and even build those relationships to determine steady state so you can understand an anomaly even when things are good.

The second thing is work with those public-private partnerships, they are so important because not only do small businesses get access to people and resources that do have million dollar budgets to do things and see more things globally, but you also put information from that 99.7 percent of the fabric back into the pot that protects the entire fabric.

We, again, only are as good as our weakest link. Our small businesses are so strong in the innovation, we can't let them be weak in the security just because of money, and we have to incentivize that spend and incentivize putting some of their resources into those partnerships.

Mr. STREBE. I believe that the most basic level, working with some of your business customers or business owners to educate them on where they can find that information is very, very crucial. I can't really speak for everybody else out there. I can speak on behalf of our credit union. We have about a thousand business accounts, and we quite often, and we have a very professional IT staff, as the Doctor suggested, that if we have a member of ours or a small business of ours that asks us how do I do this or how do I do that, while we are not in the profession of trying to give them IT security advice, we recognize the fact that without them we have no meaning, and as a small credit union or not a small credit union, we are a medium-sized or a large credit union, as a credit union, we truly believe in trying to help our membership to the greatest extent possible, so I completely agree with the Doctor that if we can provide some framework information, some construct of where they can get the information, how they can get the information and from whom, that will be very, very valuable for us going forward.

As a credit union, we will always help our membership, as I believe—while I can't speak for every credit union, I am pretty confident that I can speak for a lot of them that they would say any member of ours that wants a little bit of help in trying to understand some of the threats out there, we would definitely, definitely help them because we just feel that as a member-based organization, we need to do that.

Mr. BEAM. I would say the electric industry is a little different than some of the other small business groups in that we are currently regulated by the Federal Energy Regulatory Commission for reliability in cyber security, and so we have a clear place to go for clarification on cyber security issues. One thing I would like to emphasize as we consider new cyber security legislation is making sure you have that clear line of demarcation of one agency regulating one group and not having overlap. I think that will just cause confusion and really muddy the waters. But I would like to echo what some of the other panelists have said about the importance of the public-private partnership and the information sharing. I think that is really the key to improving our cyber security rather than through regulations.

Chairwoman ELLMERS. Excellent. Thank you so much. I am now going to recognize Ranking Member Richmond for his questions.

Mr. RICHMOND. And I think I will just start with Dr. Schneck on this. The question becomes, and we heard the Congressman talk about just general computer hygiene. If that accounts for about four out of five of the security breaches that we have, then do you think that it is worthwhile for us—or whether it has merit or it is too cost prohibitive for us—to require almost like we do with some public service announcements to remind people of these very simple things that they can do to keep their information secure. If we can cut out 80 to 85 percent just by doing that, should we require, or do you have some ways that would incentivize people to provide that information when you go to Yahoo! or whatever you do online, to provide some of that simple hygiene information and to reinforce how important that is?

Ms. SCHNECK. I absolutely agree that that basic hygiene will take care of a large percent of the issues. The analogy I would use is many years ago, Howard Schmidt used the analogy to seatbelts in cars and the process that it took to get people to use seatbelts. The other analogy that has been used is the forest fires. A lot of this goes back to education awareness that our colleagues at the NCSA do a great job of and others and certainly the credit unions that we have heard, but I want to also point out that that 20 percent is evil, that 20 percent that we can't catch with the hygiene that Representative Thornberry also mentioned. That is the part where very quiet attackers that don't want you to know that they are there, they are not looking for your bank information, they are looking to find exactly the people that sit on top of core intellectual property, whether it is recipes, oil field diagrams or diagrams for other parts, military, they will sit there until they find it, and they will send it home, and that is moving jobs, money, and markets across countries and companies, and that is the piece that we want to also incentivize companies and small companies, especially because they don't have extra money to invest in protecting that and to consider it part of the corporate risk, so I think it is twofold.

One is it certainly is an awareness campaign, and NCSA has the Cyber Security Awareness Month with the government and does a lot of different things. I think we are a lot more—I sit on the ISPAB as well, and we were briefed on some of these efforts, and I think as a community we are a lot more aware now than we were before of cyber as an issue. I think this hearing is one example of that. But the other side is these very quiet attacks. We do need to incentivize our small businesses to protect what they have. What they have is key to our national security, and that can't be overstated.

Mr. RICHMOND. Well, and part of my thinking was that if we can eliminate 60 to 80 percent strictly by information and being very creative, it would allow us and free up more money, more time, more energy to focus on those people who are going to try to do it no matter what all the time and are very sophisticated and evil with it. Anyone can answer this question, but how has cloud computing, I guess no pun intended, clouded our ability to protect ourselves? And I guess I just started to look at some of my new data in the office, and they talk about cloud computing, it just scares me

to just have information floating out there. So how safe is it, and how has it complicated your jobs and our ability to keep the country safe?

Ms. SCHNECK. I guess I will start. So the important thing is to protect data in motion, data at rest, and data in use. What cloud does is it outsources data processing, so it says that you are, to your point, you are sending your information somewhere else to be processed, and then it comes back so that you can view it, and the danger that people immediately sense is while it is not on my network and in transit and while the third party is holding it, is it protected? And these are the questions that have to get answered.

The very, very beneficial side of cloud computing is that it is very efficient. You can package your computing processing power, you can have somebody else pay the bills for chilling the computing and doing the efficiencies, you can do high performance calculation, and the data comes back and it is a fraction of a price if you had a CPU on every machine, and that scales beautifully. So for small business, you can outsource a lot of your computing needs, and it ends up saving them a lot of money.

The other side is they have to make sure when those data are in transit they are working with a third-party provider that is taking care of encrypting or protecting the identity or the data when it is in storage, when it is being processed, and certainly on its way back. A big advantage is that if you are using a good provider, whatever service it is, the high-end providers do have the million dollar budgets to secure things right, whereas the small businesses may not. So there are a lot of efficiencies and a lot of security built into cloud, even though it requires that we send our data offsite.

Mr. RICHMOND. And this question would be for Mr. Kaiser. How important is it for us to deal with breach notification laws as opposed to the many different laws in the various States, and does it make sense and would it help the small business or businesses period for us to come up with a national standard for breach notification as opposed to having different laws in I think 48 States now that have them and small businesses that do business across State line having to, I would assume, to comply with all of them.

Mr. KAISER. Yeah, I think that at the end of the day, I think wherever we can have clarity for both businesses and consumers, that is a good thing, right, so people know what to expect when something happens and know what will happen if something happens, and how that gets accomplished I think could be done probably in a number of different ways, but I do think that clarity, you know, where, you know, because the data really lives everywhere because not only of cloud, but just the way the Internet works, you know, as a consumer, I am doing business with people all over the country when I am using the Internet, and small businesses are doing business all over the country. I think where we can have clarity about what will happen when a breach occurs and from both sides, both as a person whose information was lost and also as the person or business that lost the information, I think that is just helpful in general on a lot of these cyber issues, not only that, but also on education awareness, clarity about the message, those things help. It is kind of a confusing world out there, and there is

a lot of different messages, so anything that helps that I think is good.

Mr. RICHMOND. And my last question would be for Mr. Strebe, and that question would simply be, you mentioned the analogy—the example of the liquor store that was very careless which exposed the credit union, I would assume, to I think you said \$60,000 worth of repayments. Do you think legislation—is needed to clear up responsible parties or to figure out and help find who is responsible for data breaches and who shall reimburse the consumer at the end of the day or the person who sustains the loss?

Mr. STREBE. I think with legislation you can create a framework that any small business can follow. When you look at things, we have talked about hygiene today. If they are not following simple hygiene and they are not doing a basic standard of care, I think responsibility can be held or liability can be pushed back on to a small business. If they take care of that or if they create or through legislation create a framework and create, you know, here is the exact things that you are going to do, and they follow that and they are not negligent, I think you could essentially hold them harmless for, you know, again, a due standard of care.

Anytime somebody just completely thinks that data security and cyber security is off the radar screen for them and they think that they can push all of the responsibility back to us as a financial institution, I think that creates substantial challenges for us as a financial institution. In addition, I think it is really valuable from a reputation risk standpoint to understand that anytime there is some sort of compromise and we notify our members that what has happened, they automatically think it was us as a financial institution that was penetrated, and when that happens, we have to, we spend a lot of money trying to overcome that and trying to tell them that, well, it wasn't us, we can't disclose that to you, we can't make public who it actually was, and as a result of that, those costs are borne by us.

So as I look forward, I do believe a construct or framework can create a basic standard of care that they are going to have to follow and things that they need to do, and if they are negligent in that, then they can be held responsible. You know, can you try to address every single item? I don't believe you can because, as was mentioned before, every time you try to solve one thing there are two more things that come on the horizon, and then you are just continuing to chase your tail. I just look at it and say there is some basic necessities in commerce today that have evolved over the past 10 years that a businessman really, really needs to grab hold of and make sure they are accomplishing.

Mr. RICHMOND. Thank you, and I will yield back.

Chairwoman ELLMERS. I have one more question, and I am going to quickly, and it is all for the entire panel. Of course, we are hearing about the statistics of the frequency of the cyber attacks. In general, if you could give us an idea in your sector of business what that frequency is, how often, and how often do you receive information from the Federal or State government warning you of any particular upcoming threats that might be occurring? Starting with Mr. Kaiser.

Mr. KAISER. Yeah, we don't really deal in that kind of information between the industry and government, but I will say, just as a regular person who looks at the news every day, those threats, those attacks are happening all the time, and so we really need to be able to respond to them.

Ms. SCHNECK. We see 66,000 new variants of malware every day in McAfee Labs, and that is only going up. And then if you take that and you look at the story across the sectors, those malware examples and variants are being used to do things such as steal the oil field exploration diagrams across the energy sector, and these are things that we have published.

I think you ask a very important question, how much do we get from the government? Not much right now. And that could be because of framework, it could be because of the structure. We are active in, I would say, most of the major public-private partnerships, but the idea is that we actually share a lot more out with government. When we find things, we give as much to government, law enforcement, and all the way to State and local as we can, and looking at how we can do that more quickly, take the most actionable egregious information and get it to law enforcement faster is a challenge across, I believe, the entire business community, and the way this affects small business is that needs to get to them, and we are legally tied when it comes to sharing with the private sector. It is a little bit easier in some cases with government, but we need to get it back to those small businesses, and that is why from personal experience, I advocate that small businesses get with those partnerships.

Mr. STREBE. In our case I cannot give you specific numbers. What I can tell you is, as a financial institution, we do this 24/7/365 times, however many years are in the future. We always have to do this. We are getting, I don't want to say hit, because that sounds like somebody actually penetrates us. We always see—we have a fortress or a cyber fortress that is built around our financial institution, and we always see people coming from all around the world trying to find vulnerabilities in our system and IP addresses that are open and they can try to penetrate our system. 24/7/365 times the future, that is exactly how many times we see it. It is always happening.

Mr. BEAM. As far as notifications from the government, NERC has a advisory system where they send out alerts. We have received 40 of those since 2008. Of those, the majority were advisories that were just advising us of a potential issue. Only a handful were things that required us to take action, but we did take action on those, and none of those was an imminent threat. They were a potential threat that you needed to take action to prevent.

On the business side, we have our system divided into two completely separate networks. One controls the electric system, and one is the business system. The electric system is completely separate from the Internet. There is no connection. And so we have had no outside traffic ever able to get on to that system and cause any kind of malicious attack.

On the other side, in 2011 alone, we got 74 million emails hit the firewall. Of those, only 16 million got through, and those in our in-

ternal review processes only allowed 4 million through to the actual end users as legitimate emails. So as everybody else has said, we are constantly getting things that are malicious in one way or another, be it spam or whatever, but they are not necessarily attacks from a foreign government of that type. As far as anything that was actually directed to the electric system in a malicious way, we have never had an attack that we are aware of.

Chairwoman ELLMERS. Mr. Strebe, have you in your industry, in the financial credit union world, does the Federal or State level of government, do you get notifications that there are imminent threats?

Mr. STREBE. If I waited until I got the information from them, it would be way too late.

Chairwoman ELLMERS. So you are on top of it ahead of time?

Mr. STREBE. We quite often end up sharing what is happening in our institution with other folks that are out there, yeah. We can't wait. We know before everybody else does because it is real time for us.

Chairwoman ELLMERS. Thank you, thank you. I just wanted to make sure I clarified that.

And again, thank you to all of our participants, you know, panel 1 and panel 2. This subcommittee will continue to closely follow this issue. I want you to be aware of that and know that we are going to be working on this very issue. It is clear that there is no one-size-fits-all policy for cyber security. I look forward to working with my colleagues to make sure small businesses have the resources available to combat cyber attacks while not adding to any duplicative regulatory burdens.

I ask unanimous consent that Members have 5 legislative days to submit statements and supporting materials for the record. Without objection, so ordered. This hearing is now adjourned. [Whereupon, at 2:26 p.m., the subcommittee was adjourned.]

**Statement Of
Rep. Mac Thornberry (TX-13)**

Before The

**House Committee On Small Business
Subcommittee On Healthcare and Technology
United States House Of Representatives**

December 1, 2011

Chairwoman Ellmers, Ranking Member Richmond, and Members of the Subcommittee, I appreciate the opportunity to offer some thoughts today about cybersecurity.

Cybersecurity is a complex set of issues that touches nearly every aspect of our lives. It is not only about national security, but also job creation and our economy. Every day, businesses of all sizes are targeted for their intellectual property – things like blueprints, formulas, and business plans. When information is stolen from U.S. databases, jobs are stolen from the U.S. economy.

We even hear stories of small businesses developing a new product, being hacked, and finding copies of their new products hitting the market at cut-rate prices from overseas countries within a few months. This is a direct threat to our global competitiveness.

Every day most of us take common-sense precautions about our personal safety and valuables. We lock our doors; we keep our cash in a safe place; we do not give out our bank account or Social Security numbers to anyone we do not trust. Yet, too many of us do not take such precautions in one of the most dangerous places where many go every day — cyberspace.

Earlier this year, U.S. House Speaker John Boehner and Majority Leader Eric Cantor asked me to lead a Task Force to make recommendations on what Congress could do right away to deal with this problem. The goal was not to develop legislation, but to make

recommendations that provide a framework for the committees to write and pass legislation during this Congress that will make a real difference in cyber.

Part of the reason that little progress has been made is that cybersecurity is a complex issue that cuts across jurisdictions and turf in both the legislative and executive branches of government. The Task Force, made up of 12 Members representing 9 different committees and 3 at-large Members, enabled us to get past many of the jurisdictional hurdles by getting everyone in the same room to talk cybersecurity. Each committee was able to hear the different perspectives and approaches from other committees, which went a long way in gaining a better view of the challenges that we face.

The Task Force recommendations were delivered to Leadership and released publicly in early October of this year. Although there are many specific recommendations covering a variety of issues, generally there were two main areas that we felt would have the most impact on cybersecurity moving forward.

The first area the Task Force believes that Congress should act upon is to promote a series of incentives to help raise the level of cybersecurity generally and increase awareness. Estimates are that 85 percent of threats in cyberspace can be eliminated with proper cybersecurity “hygiene.” Raising the awareness of cybersecurity to C-level executives and small business owners will help companies put in place the technology and good practices that are already available to reduce cyber attacks.

The second area is to address the more sophisticated attacks from large groups and state actors by increasing information sharing between the federal government and private businesses as well as getting companies to share more with each other. To allow this type of information

sharing for new and existing partnerships, we identified a series of laws that have not kept pace with advancements in technology that need to be updated. We also felt it was necessary to create an entity that is run and operated outside of government to act as a clearinghouse of information. By involving Internet Services Providers (ISPs) and plugging in the classified information of the federal government, this type of entity could move towards “active defense,” where cyber attacks are blocked or quarantined before they even reach a company. This approach is similar to the 90-Day Defense Industrial Base (DIB) Pilot Program where ISPs use classified information from the federal government to help protect the networks of the DIB participants.

These recommendations and the others in the Task Force report will not solve all of the challenges we face with cybersecurity. However, they do offer a framework for us to move forward this Congress and increase cybersecurity protections for small businesses and our country.

Again, thank you for holding this hearing and allowing me to offer my thoughts.

**Statement of the North Carolina Electric Membership Corporation
to the United States House of Representatives
Committee on Small Business, Subcommittee on Healthcare and Technology**

Hearing on Cybersecurity

December 1, 2011

Executive Summary

Electric cooperatives (co-ops) worked with Congress, the Federal Energy Regulatory Commission (FERC) and its industry counterparts to ensure that the 2005 Energy Policy Act (EPAAct) contained strong and effective reliability provisions aimed at protecting the Bulk Power System (BPS), also called “the grid.” Co-ops actively participated in the formation and development of the industry reliability self-regulatory organization, the North American Electric Reliability Corporation (NERC). Six years later, co-ops are deeply engaged in the development of NERC’s reliability standards, including the cybersecurity standards.

North Carolina Electric Membership Corporation (NCEMC) is a “registered entity” on the NERC Compliance Registry because of the size and function of some of its transmission and generation assets. It also handles NERC compliance for some of the distribution cooperatives which collectively own NCEMC. NCEMC has first-hand experience with the responsibilities and burdens related to creating and implementing a functional set of reliability and cybersecurity standards.

Like all cooperatives, NCEMC takes its responsibility to protect the grid very seriously. NCEMC recognizes that reliable electric service and national security are both of paramount importance. Multiple discussions are taking place in Congress and within the Administration about how to increase cybersecurity protections for critical infrastructure. NCEMC and NRECA commend the work of Speaker John Boehner’s Cybersecurity Task Force and the leadership of Rep. Mac Thornberry.

NCEMC and its national trade association, the National Rural Electric Cooperative Association (NRECA), believe the NERC process is working well. The process could be

strengthened by narrowly targeted legislation that 1) provides the federal government the ability to react quickly to severe, imminent cyber threats and 2) increases the amount of timely, actionable information flowing to grid owners and operators. The scope of any proposed legislation should be limited to those assets and systems which are realistic targets of a cyber threat and which could have significant impact on the security of the BPS. Casting too wide a net could bring entities like distribution co-ops and other small businesses under potentially very burdensome regulatory requirements with little or no benefit to grid security.

Introduction

Chairman Ellmers and Ranking Member Richmond, and all members of the Subcommittee, thank you for the opportunity to testify today on electric cooperatives' responsibilities to provide cybersecurity protections to one of the nation's most critical infrastructures, the bulk power system, also known as "the grid." My name is David Beam and I am Senior Vice-President, Corporate Strategy, at NCEMC. As the corporate compliance officer for NCEMC, I have oversight responsibilities in the areas of energy risk management and regulatory compliance. In this capacity, I am the senior manager responsible for NERC reliability compliance and cyber security. I bring over 30 years experience in the electric utility industry to these roles.

While my testimony and remarks today are made on behalf of NCEMC, I would also like to briefly mention the National Rural Electric Cooperative Association. NRECA is a trade association consisting of over 900 cooperatives providing electricity to 42 million consumers in 47 states. As member-owned, not-for-profit organizations, cooperatives have an obligation to provide a reliable supply of electricity to all consumers in our service areas at the lowest possible

price. Cooperatives serve primarily the more sparsely populated parts of our nation but cover roughly 75 percent of the nation's land mass and maintain 42 percent of the nation's electric distribution lines. All but five of the nation's distribution electric cooperatives are considered small businesses under guidelines set by the Small Business Administration¹. All of the distribution cooperatives that own NCEMC are small businesses.

In my testimony today I hope to achieve the following:

1. Provide a basic explanation of the Bulk Power System and how it differs from and is isolated from the distribution system.
2. Offer some background on the Energy Policy Act of 2005 and the purposes of NERC to help explain the origins of the cybersecurity regime NCEMC complies with today.
3. Share information about how NCEMC works to achieve a culture of compliance with the NERC standards and industry cybersecurity best practices.
4. Contribute NCEMC's and NRECA's general views on the state of cybersecurity legislation and the potential impact of new legislation.

The Bulk Power System and the Distribution System

The U.S. has three major bulk power systems or grids: (a) the Eastern Interconnect, consisting of the eastern two-thirds of the United States; (b) the Western Interconnect, consisting primarily of the Southwest and areas west of the Rocky Mountains; and (c) ERCOT, consisting mainly of Texas. NCEMC resides in the Eastern Interconnect.

¹ Annual retail sales of less than four million megawatt hours of electricity.



(Map obtained from the Energy Information Administration)

Generally speaking, NERC standards apply to the BPS, which NERC standards refer to as the “bulk electric system.” NERC’s general definition of the bulk electric system is “as defined by the regional reliability organization², the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition. A bulk power system consists of high-voltage connections between individual utilities designed to permit the transfer of electrical energy from one part of the network to another.” NERC, its regional entities and an industry standards drafting team are currently engaged in a process to revise the BES definition.

Contrary to popular belief, a remote hacker cannot easily access the telecommunications systems that overlay parts of the bulk power system. Utilities employ multiple layers of defenses and ensure that the telecommunications systems used to operate the generation and transmission assets are separate and distinct from the telecommunications systems that are visible to the public. The types of defenses employed by NCEMC are described in more detail in the “NCEMC Cybersecurity Operations” section of this testimony.

The electric industry has deep experience with assessing and mitigating a wide variety of threats to critical infrastructure assets. For example, we’ve restored power after hurricanes and ice storms for decades. Electric utilities have focused on cyber threats increasingly over time, in

² NCEMC is part of the Southeastern Reliability Corporation (SERC).

proportion to the increasing use of automated components in generation, transmission and distribution of electricity. It is important to note that each utility has a mix of older and newer equipment. Many parts of the bulk power system operating today still rely on mechanical components that are not programmable; in many cases these older assets are not vulnerable to cyber threats.

Distribution utilities receive power from the bulk power system and transmit it to retail customers. Because outages at the distribution level cannot cascade back up to the bulk power system, NERC standards do not generally cover distribution lines and substations. However, with the advent of the smart grid and increasing installations of smart meters across distribution systems, electric cooperative member-consumers are asking questions about the cybersecurity of telecommunications-enabled components in smart meters and appliances. In acknowledgement of the consumer interest in security protections for their utility usage data and communications with their electric service provider, NRECA, through its Cooperative Research Network (CRN), has developed a “Guide to Developing a Cyber Security and Risk Mitigation Plan.” Using these tools cooperatives (and other utilities) can start immediately to strengthen their security posture and chart a path of continuous improvement. The plan includes:

1. **Cyber Security Risk Mitigation Checklist.** A list of activities/security controls necessary to implement a cyber security plan, with rationales.
2. **Security Questions for Smart Grid Vendors.** CRN is encouraging co-ops to include these questions in their RFPs for smart grid components. The questions are designed to facilitate a frank and open dialogue on cyber security with those who make and sell components.

3. **Interoperability and Cyber Security Plan.** The Interoperability and Cyber Security Plan (ICSP) examines risk management, identification of critical cyber assets, and electronic security perimeters, among other issues.

Existing NERC Procedures Guide Industry through Threats and Vulnerabilities

In order to increase the protection afforded to the bulk power systems or grids, throughout the country, Congress approved a mandatory and enforceable reliability standards regime for the bulk power system in the Energy Policy Act of 2005. It is commonly referred to as “Section 215” because it resides in Section 215 of the Federal Power Act. Under Section 215, NERC employs a stakeholder-driven process involving electric power industry experts, regional entities, Federal Energy Regulatory Commission (FERC) staff and other government representatives, to draft mandatory and enforceable reliability and cyber security standards that apply across the North American grid.

When it comes to reliability issues, the investor-owned, municipal, cooperatively-owned and merchant sectors of the electric power industry work closely together in many forums. Regardless of ownership structure, utilities dedicate thousands of employee hours to the standards development process and routinely share information through NERC and other discussion forums. I am personally involved in standards development and policy through my role as a member of the SERC Board Executive Committee. NCEMC staff work with other utilities through SERC committees, NRECA and other forums to review and provide input into industry standards.

Section 215 has a stakeholder-driven process because electric utility owners and operators are experienced and knowledgeable about how to provide reliable electric service at a

reasonable cost to our customers, and we understand how our complex systems are designed and operated. We are uniquely positioned to understand the consequences of a potential malicious act and the proposed mitigating actions needed to prevent such exploitation, including ensuring against unintended consequences of remedial actions.

FERC has the authority to approve or remand standards that emerge from the stakeholder process. NERC and FERC can levy fines on utilities that violate the standards and have done so. Additionally, FERC can direct NERC to develop new or revised reliability standards within a specific timeframe. The reliability standards cover physical and cyber aspects of the grid. The self-regulatory structure and level of industry investment in the ERO provide the means to improve and revise existing procedures and reliability standards to address additional threats and vulnerabilities.

NERC also has authority to distribute alerts on topics that are important for industry to address. There are three levels of alerts: Advisory, Recommended Action and - the most critical advisory level - Essential Action. Recommended Action and Essential Action Alerts have mandatory reporting requirements that typically demonstrate what action an entity has taken. NERC and the industry have used the alert process successfully to distribute critical information related to many issues, including Aurora, Stuxnet, Night Dragon, geomagnetic disturbances and many other cyber and operational issues.

NCEMC Asset Overview

NCEMC is a generation and transmission cooperative that provides wholesale power and other related services to 25 of the 26 electric cooperatives incorporated in the state of North Carolina. For 20 of the cooperatives, called Participating Members (PMs), NCEMC is the full

requirements power supplier. For 5 of the cooperatives, called Independent Members (IMs), NCEMC provides partial requirements capacity and energy entitlements from designated resources, pursuant to a Wholesale Power Supply Agreement. The twenty-sixth cooperative, French Broad EMC, is not a member of NCEMC.

The service territories of NCEMC's member distribution EMCs are located within the balancing areas of Progress Energy Carolinas ("PEC"), Duke Energy Carolinas ("Duke Energy"), and PJM Interconnection LLC³ ("PJM"). Therefore, NCEMC's system consists of three distinct areas, identified as supply areas, located entirely in the state of North Carolina.

NCEMC is registered as the responsible entity for reliability and cyber-security compliance for its own assets as well as those of its Participating Members. These assets include generation and transmission facilities and associated protection equipment and procedures.

NCEMC relies on the transmission systems of Duke Energy, Progress Energy and PJM to transfer the power it generates and purchases to the 198 delivery points of the PMs; 125 in Progress, 46 in Dominion, and 27 in Duke. 151 of those are Transmission delivery points and 47 are Distribution. NCEMC's all-time peak load was 3232 MWs at generation in December, 2010. NCEMC and its members own roughly 17 miles of 230kV transmission lines along with a large amount of 115kV transmission. All of these facilities are radial, load-serving transmission with one source. In addition, NCEMC's members operate extensive distribution systems which deliver power to retail consumers, but are not part of the BES.

Since 1980, NCEMC has been a part owner in the baseload Catawba Nuclear Station located in York County, South Carolina. Duke Energy operates and maintains the station, which has been operational since 1985. NCEMC's ownership share consists of 61.51 percent of Unit 1,

³ The PJM Interconnection is a regional transmission organization (RTO) that coordinates the movement of wholesale power in 13 states, including North Carolina. It operates a competitive wholesale market and manages the high-voltage electricity grid.

approximately 704 MW (1,145-MW unit capacity) and 30.754 percent in the common support facilities of the station. NCEMC's ownership entitlement is guaranteed through a reliability exchange between the Catawba Nuclear Station and the McGuire Nuclear Station located in Mecklenburg County, North Carolina. The reliability exchange results in an effective guaranteed capacity of 681.9 MW.

NCEMC owns and operates 622 MW of aero-derivative combustion turbines on a site in Anson County and a site in Richmond County, both in North Carolina. These peaking resources operate on natural gas as primary fuel, with diesel storage on-site as a secondary fuel. These units have been in commercial operation since 2007.

NCEMC also owns and operates two internal-combustion, diesel-powered generating stations on the Outer Banks of North Carolina (located on Ocracoke Island and in Buxton). These super peak units, which began commercial operation in 1991, have a combined capacity of 18 MW and are used primarily for peak shaving and voltage support.

NCEMC Cybersecurity Operations

Compliance Organizational Overview

NCEMC follows exacting procedures to ensure compliance with NERC standards. The NCEMC Board of Directors has approved a compliance policy that affirms NCEMC's on-going commitment to oversee compliance with applicable state and federal laws and regulations and authorizes the establishment of a formal compliance program. The comprehensive Compliance Program is intended to foster awareness and commitment to compliance by all employees, provide for effective preventative measures to discourage non-compliance, facilitate prompt detection, cessation and reporting of violations, and establish effective remediation measures should violations occur.

NCEMC has devoted significant financial and human resources to assuring reliability and cybersecurity. As mentioned above, I serve as the NCEMC Compliance Officer, overseeing all our reliability and cybersecurity compliance activities. In addition, I serve on the SERC Board of Directors and Board Executive Committee, where I am in a position to monitor and provide input to the compliance enforcement process. NCEMC has employed a full time compliance coordinator, whose sole responsibility is to manage compliance with reliability and cybersecurity standards. In addition, NCEMC employs a compliance team of subject matter experts (SMEs) who have individual responsibility for compliance with their assigned cybersecurity and reliability standards. The SMEs are also engaged in the standards process through participation on various SERC committees, the NERC standards process and through NRECA. . NCEMC also utilizes the services of outside contractors to audit and provide recommendations for improving our reliability and cybersecurity compliance. Additionally, there is at least one employee at each of NCEMC's Members who is assigned responsibility for compliance with reliability and cybersecurity standards.

The Compliance Program lays out a general structure for managing compliance with all corporate compliance obligations. Oversight for each compliance function is assigned to a Compliance Manager. A separate, written Compliance Plan is established for each compliance function laying out specific processes and procedures for ensuring compliance consistent with principles outlined in the Compliance Program.

The Compliance Plan lays out the structure, processes and procedures for managing compliance with all applicable reliability and cybersecurity standards. The Compliance Plan was developed by the Compliance Manager and the Compliance Team, with oversight from the

Compliance Officer. The final Compliance Plan was reviewed by senior management and approved by the Compliance Officer.

The NERC Compliance Plan undergoes an annual program review conducted by the Compliance Manager, the Compliance Team and the SMEs. As part of this process, the plan is reviewed for any opportunities for improvement and the Compliance Manager recommends any changes or additions. Any recommended changes are reviewed and approved by the Compliance Officer.

Cyber Security Technology Overview

NCEMC has made significant technology investments in order to assure compliance with NERC cybersecurity standards. Some are just common sense and would be best practices even without the standards. For example, users are required to change password every 90 days and our data center is secured via the electronic badge access. Access to our data center is logged.

Other measures are more involved and costly. For example, NCEMC operates two autonomous networks - a secure network for business systems and a secure network for Energy Management Systems (EMS). No internet traffic (email, word processing etc.) is allowed on the EMS network. Remote access into the EMS network is monitored and controlled through Virtual Private Network. Each access granted has to be requested and authorized before use and terminated as soon as the job is complete. All the remote access is logged and monitored.

Looking even more closely at NCEMC's efforts, Security Event Incident Management (SEIM) systems are used to proactively monitor networks "24x7x365" for anomalies and unauthorized access. Firewalls are used at the internal and external network access points.

Substation communications are used to collect telemetry data but no command and control is available for the substations.

Finally, to document adequately that NCEMC has complied with all the substantive NERC requirements, NCEMC employees spend a great deal of time performing regular testing of the systems and processes described above. We conduct an annual disaster recovery test to ensure our ability to promptly recover all critical systems in the event of a major event. We also perform rigorous audits internally and pay external firms for regular audits. SERC may audit our compliance at any time.

Viewpoints on Future Cybersecurity Legislative Proposals

Since cybersecurity threats are constantly evolving, the electric cooperative sector recognizes the potential for some threats so imminent and severe that even the comprehensive, carefully designed NERC procedures and standards cannot assure the timely distribution of information and direction to industry to achieve an adequate industry response to protect the bulk electric system. In those limited circumstances, when the President of the United States has determined that emergency action is warranted, the federal government should have the authority to issue orders that directly address the threat and the necessary mitigation actions needed to protect the bulk power system. Electric cooperatives, along with the entire electric power industry, have supported this additional limited authority for over three years.

However, any future legislation seeking to create new authorities that largely duplicate existing FERC authority under Section 215 of the Federal Power Act could substantially undermine the existing reliability standards regime. This is most likely to occur if legislation

emerges seeking to provide additional FERC authority to write standards or issue orders concerning grid vulnerabilities⁴, as opposed to imminent threats.

When addressing cybersecurity, we encourage Congress to focus its attention on the immediate, narrow issues at hand: 1) the need for the federal government to issue emergency orders very quickly if the bulk power system is under an imminent threat of cyber attack; and 2) the need for the electric power industry to hold more security clearances in order to better facilitate the sharing of timely, actionable information needed to fashion responses to such threats. The scope of any proposed legislation should be limited to those assets and systems which are realistic targets of a cyber threat and which could have significant impact on the security of the BPS. Casting too wide a net would bring entities like distribution co-ops and other small businesses under potentially very burdensome regulatory requirements with little or no benefit to grid security.

NCEMC and NRECA agree with and appreciate the observations and recommendations issued in Speaker Boehner's Cybersecurity Task Force Report (Oct. 2011), including:

- *"Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity at these facilities using existing regulators." (p. 9)*
- *"Industries with identified critical infrastructures should have full and complete participation in the development of cybersecurity standards and best practices. (p. 9)*
- *"The Department of Homeland Security should work with other regulators to help coordinate security standards across sectors" (p. 9)*
- *"... [G]reater sharing of information is needed within industries, among industries and between government and industry in order to improve cybersecurity and to prevent and respond to rapidly changing threats." (p. 10)*

⁴ Vulnerabilities are potential weaknesses which could be exploited to attack the grid. However, vulnerabilities typically have longer lead times and do not pose an immediate threat. The NERC-FERC regime as it exists today has guided the electric sector through multiple vulnerabilities, as noted above in my testimony.

Conclusion

Thank you for the opportunity to testify at today's important hearing. I appreciate the opportunity to discuss cybersecurity issues with the members of the House Small Business Subcommittee on Health and Technology. NCEMC and NRECA are ready, willing and able to serve as a resource on this issue which has the potential to impact our grid, economy and national security.



Testimony of

Glenn Strebe

President/CEO of Air Academy Federal Credit Union

On behalf of

The National Association of Federal Credit Unions

“Cyber Security”

Before the

House Small Business Committee

Subcommittee on Healthcare and Technology

United States House of Representatives

December 1, 2011

Introduction

Good afternoon, Chairwoman Ellmers, Ranking Member Richmond and Members of the Subcommittee. My name is Glenn Strebe, and I am testifying today on behalf of the National Association of Federal Credit Unions (NAFCU). Thank you for holding this important hearing. I appreciate the opportunity to share my views on cyber security and data security at our nation's credit unions.

I received my Bachelor of Science degree from the United States Air Force Academy and an Master's in Business Administration from Colorado State University. Since 1998, I have served as the President and CEO of Air Academy Federal Credit Union, headquartered in Colorado Springs, CO. AAFCU has \$420 million in assets and serves more than 42,000 members in our 9 locations, as well as in student operated branches at two high schools. Previously, I served AAFCU's membership as the Chief Operating Officer and Chief Financial Officer. Prior to joining the credit union, I was an auditor and a financial analyst in the United States Air Force.

NAFCU is the only national organization that exclusively represents the interests of the nation's federally chartered credit unions. NAFCU is comprised of over 800 member-owned and operated federal credit unions. NAFCU member credit unions collectively account for approximately 62 percent of the assets of all federally chartered credit unions. NAFCU and the entire credit union community appreciate the opportunity to participate in this discussion on data security.

Background on Credit Unions

Historically, credit unions have served a unique function in the delivery of necessary financial services to Americans, including making business loans. Established by an Act of Congress in 1934, the federal credit union system was created—and has been widely recognized—as a way to promote thrift and to make financial services available to all Americans, including small businesses, who would otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to fill a precise public need—a niche that credit unions fill today for nearly 93 million Americans.

Every credit union is a cooperative institution organized “for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes.” (12 U.S.C. §1752(1)). While more than 75 years have passed since the *Federal Credit Union Act* (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- Credit unions remain singularly committed to providing their members with efficient, low cost, personal service; and,
- Credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

The nation’s approximately 7,200 federally insured credit unions serve a different purpose and have a fundamentally different structure than banks. Credit unions exist solely for the purpose of providing financial services to their members—while banks strive to make a profit for their shareholders, while also serving their customers. As owners of cooperative financial institutions

united by a common bond, all credit union members have an equal say in the operation of their credit union—“one member, one vote”—regardless of the dollar amount they have on account. These singular rights extend all the way from making basic operating decisions to electing the board of directors. Federal credit union directors also generally serve without remuneration—epitomizing the true “volunteer spirit” permeating the credit union community.

Today, credit unions continue to play a very important role in the lives of millions of Americans from all walks of life. As consolidation among financial depository institutions has progressed with the resulting de-personalization in the delivery of financial services by some large banks, the emphasis in consumers’ minds has begun to shift not only to services provided but also—and in many cases more importantly—to quality and cost. While many large banks have increased their fees and curtailed customer service as of late, credit unions continue to provide their members with high quality personal service at the lowest possible cost. This has been evidenced most recently as thousands of Americans turned to local credit unions after several large national banks proposed new fee increases.

Protecting Consumer Information

NAFCU supports efforts to enact comprehensive data and cyber security measures to protect consumers’ personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act (GLBA). Unfortunately, there is no comprehensive regulatory structure similar to what was put in place for financial institutions under GLBA for other entities that may handle sensitive personal and financial data. While NAFCU supports new measures to combat data breaches, any new legislation should

create a safe harbor for financial institutions already in compliance with GLBA; failing to do so would place an undue burden and cost on financial institutions that would be forced to retool systems that they already have in place.

Consistent with Section 501 of GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among financial institutions. The best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. By and large, financial institutions, especially credit unions, have not been the source of significant data breaches. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

A Closer Look at the Gramm-Leach-Bliley Act

GLBA helped establish the current standard for financial institution consumer data privacy. GLBA places restrictions on the ability of financial institutions to share nonpublic personal information with nonaffiliated third parties. Under the Act, the definition of financial institution includes any entity offering financial products, including banks, insurance companies, securities houses, and credit unions. It should be noted that the GLBA was enacted at the dawn of the internet age, before many online payment systems became popular and, thus, not all are covered under this definition.

Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.
- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

The Act also imposed an affirmative obligation on financial institutions to respect their customers' privacy interests. In general, the Act permits financial institutions to share information with third parties selling financial products (e.g., insurance or securities) provided certain requirements are met. Financial institutions may continue such joint marketing practices without being subject to opt-out provisions of the legislation, provided they disclose the practice to their consumers and members and enter into a confidentiality agreement with the third party.

GLBA requires credit unions to provide clear and conspicuous privacy notices to members. The language must be understandable and written in a manner to let the reader know the purpose and significance of the notice. Furthermore, the privacy notices must accurately reflect the practices of the credit union. These annual privacy notices constitute a major compliance cost.

State laws are not superseded, altered, or affected, except to the extent that it is inconsistent with the federal privacy regulations. A state statute, regulation, etc., is deemed consistent with the privacy regulations if the FTC determines that it provides a consumer greater protection than those provided under the privacy regulations. For all practical purposes, a more protective state law will supersede GLBA protections.

Pursuant to section 508 of GLBA, the Treasury conducted a study of information sharing practices among financial institutions and their affiliates and came to five general conclusions:

- First, financial services providers and their customers have a strong interest in promoting the security of personal financial information that is following prudent practices so that information is used for the benefit rather than the harm of the customer.

- Second, the sharing of information, within secure parameters reinforced by uniform national standards, has increased the access of more consumers to a wider variety of financial services, at lower costs, than ever before.
- Third, the growing problem of fraud through identity theft not only disrupts the lives of individuals and families, but it also tears at the fabric of commerce in our information age.
- Fourth, in our technology-based economy, so dependent upon accurate, timely information, current uniform national standards for information sharing have proven as essential to fighting identity theft as they are for economic growth and prosperity.
- Fifth, customers need to understand more easily and clearly the information-sharing practices of their financial institutions and how to exercise their say in how that information is shared in support of the customer relationship.

The GLBA addresses a number of key aspects of data security as outlined below.

Sensitive Consumer Information

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log onto or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

An information security program must begin with a comprehensive risk assessment to ensure that the policies, procedures and controls used to accomplish the institution's information security and privacy goals have enough depth and breadth to reach every impacted area within the organization. Technological solutions may represent part, or all, of the program depending on the needs of the institution. Such technological solutions may include two-factor authentication of user identities; firewalls and virus management strategies, error logs monitored continuously for attacks and attempted attacks.

Risk Assessment and Controls

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

It is imperative that institutions understand that internal threats often times pose more of a threat to the institution and its members than hackers from the outside. With this in mind, the institution ensures strong hiring verification practices and incorporates training programs to promote a culture of compliance among its staff. At Air Academy Federal Credit Union, we have a number of internal control tests that we perform to train our employees on how to handle situations such as someone coming in dressed as a repairman trying to gain access to our server room.

Other issues are also important. For example, record retention, storage, and destruction is rapidly finding its way to the top of the compliance risk matrix. Similarly, business upgrades to their PCs have led to mass abandonment of computers whose files and hard drives not been sufficiently scrubbed to ensure data is irretrievable. Failure to adequately protect a member's identity when disposing of old records and/or old equipment may result in significant legal and compliance repercussions.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business.

At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information; and,
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Train staff to implement the credit union's information security program.
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.”

Service Providers

The security guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to,

or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers

Components of a Response Program

At a minimum, an institution's response program should contain procedures for the following:

- Assessing the nature and scope of an incident, and identifying what consumer information systems and types of consumer information have been accessed or misused
- Notifying its primary Federal regulator as soon as possible after the institution becomes aware of an incident involving unauthorized access to or use of sensitive consumer information, as defined below;
- Consistent with the agencies' suspicious activity report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
- Taking appropriate steps to contain and control the incident to prevent unauthorized access to or use of consumer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and,
- Notifying customers or members when warranted.

Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable

the institution's members to take steps to protect themselves against the consequences of identity theft.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

Data Security at Air Academy Federal Credit Union

At Air Academy Federal Credit Union (AAFCU) we are relentless in our efforts to protect our members' sensitive data. The increased reliance on internet-based services has created new challenges and expenses over the last decade. With over 10,000 of our members living out-of-state, a large number of our transactions are performed online. In order to address this growing

trend, AAFCU has implemented and continues to execute security measures on many different levels. The following is a list of security components we use at AAFCU:

1. Firewall
2. Intrusion Prevention
3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email
12. Encryption
13. End point security

Associated costs for Info Security Components:

1. Firewall, Intrusion Detection & Prevention (IPS/IDS) and Botnet Filtering: \$4,000 annually for maintenance support. Initial procurement: \$37,000;
2. 24/7 Monitoring of firewall; IPS/IDS and Botnet Filtering: \$2900 monthly;
3. Firewall and server log collection/monitoring: Initial procurement: \$33,500; support renewals: \$5,000 annually;
4. Secure email and encryption: Initial procurement: \$94,000; subsequent upgrades and maintenance since 2003: \$81,000 (about \$10,000 annually);
5. Anti-Virus and Malware protection: \$3,000 annually;
6. End-point security and laptop encryption: \$1500 annually;
7. Phishing take down services: \$9,995 annually;
8. Web and Spam filters: \$5,000 annually; and
9. Third party vulnerability and penetration testing: \$100,000 annually.

At AAFCU, we take our cyber security seriously. We use an “ethical hacker” that tests our security measures, looking for hidden vulnerabilities that need repair. All of our laptops and thumb-drives that are used on our systems are encrypted in case they ever fall into the wrong hands. We like to change penetration testing vendors as well as service providers every 2 to 3 years in order to avoid complacency and to keep a “fresh set of eyes” on our security system.

While all of these steps have a cost, we view them as best practices, especially for an entity that is serious about protecting their members' data.

For the record, our system has never been successfully hacked, and from our side, none of our members' sensitive data has ever been accessed by anyone without authorization. But despite much effort and expense to protect our members' sensitive data, the same information is routinely held by other entities that do not take the protection of sensitive data as seriously. Because the sensitive data is only as safe as the weakest link provides for, our members' data is often still vulnerable to hackers and thieves through the inadequate security systems of merchants, retailers, or other entities that store this type of consumer data.

The following is a list of estimated compromise totals within the last couple of years:

- 2009 – Cheers Liquors – over 200 cards involved – losses were just over \$60,000.
- 2010 – Valero/Gas Stations – over 1600 cards involved – losses were just over \$85,000.
- 2010/2011 – Michael's Store – over 200 cards involved – losses were just over \$20,000.

In late 2010, we began to receive debit card compromise notices due to a data breach at the TJ Maxx/Home Goods database. In total, we had 3,100 member debit cards listed in the various compromise alerts. Over 2,000 letters were mailed out to members and we ultimately reissued 1,700 plastic cards. We calculated our expenses from this compromise (excluding labor) to be approximately \$4,000.

Visa and TJX announced an alternative recovery program to help issuers to quickly and easily offset the costs incurred with this compromise. TJX will pay \$41 million to Visa to fund this program. Our calculated settlement offer came to \$1,370 – about 35% of our incurred expenses. Given the time and effort required to litigate directly against TJX, we will likely accept this settlement. Payment is contingent upon 80% of the issuer's accepting their respective offers. I imagine the vast majority will take the money and put the issue to rest.

Data Breach/Notification Proposals and Recommendations

Data breaches are a serious problem for both consumers and businesses. Financial institutions such as credit unions also bear a significant burden as they incur steep losses in order to reestablish member safety after a data breach occurs. The number and scope of data breaches are significant, and the damage realized is surprising.

For example, in 2009, the Heartland Payments Systems, a company that processes card payments for restaurants, retailers, and other merchants, disclosed that the computer the company used to process transactions had been compromised. Customer records for over 100 million payment card transactions per month, at nearly 175,000 merchants, were stolen. Millions of American consumers instantly became victims. Other infamous data breaches include an estimated 4.2 million credit and debit card numbers stolen from Hannaford Bros. grocery stores in the New England area in 2008, and retail giant TJX losing 94 million customer records in 2007.

More recently, on May 11, 2011, Michaels Stores, Inc. notified its customers that more than 90 terminals in 20 different states had been compromised in a debit card PIN scheme that may have compromised tens of thousands of customers' debit cards. This breach has been linked to hundreds of thousands of dollars in fraudulent cash withdrawals in California alone.

The emotional toll that a data breach can take on consumers is immense. Information and identities can be stolen, fraudulent account charges can occur, and credit scores can be damaged. Along with consumers, small financial institutions like credit unions also face financial burdens when fraud occurs. Credit unions are often forced to charge off fraud losses, which often stem from the failure of merchants to protect sensitive financial information about their customers or the illegal maintenance of such information in their systems.

In cases of data breaches or fraud, as demonstrated by the Michaels Stores breach discussed above, it is the credit union that must notify its members, issue new cards, change account numbers, and perform a host of other activities, all of which cost both time and money. The merchant who failed to protect the data is often undisclosed and unknown to the consumer and does not pay to make the consumer whole. Interchange fees have historically been one way the costs of such breaches were offset by merchants. However, recent Congressional action to limit debit interchange fees does not fully recognize this problem and will result in heavier burdens falling on financial institutions and consumers. Understanding the significance of debit

interchange to help offset data breaches at the hands of retailers and other entities that handle the same types of consumer information as financial institutions is critical.

Meanwhile, as cases of fraud become more prevalent, costs that credit unions pay for insurance, prevention services, and staff to handle member concerns continues to grow. As the volume of plastic card usage increases, so does the risk of data breaches and fraud.

The GLBA has worked for financial institutions and should serve as a model to extending greater data protections to other entities. In addition to complying with the GLBA, credit unions have been known to go above and beyond in helping their members navigate the steps they should take if they have been the victims of fraud. It should again be noted that there is no comprehensive regulatory structure similar to the GLBA for retailers, merchants, or others who collect or hold sensitive information.

NAFCU continues to seek enactment of comprehensive data security legislation in the 112th Congress and beyond. In the House, Rep. Mary Bono Mack (R-CA), Chairwoman of the Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade, introduced the *Secure and Fortify Electronic Data Act (H.R. 2577)*. The bill awaits action by the full committee. In the Senate, Tom Carper (D-DE) and Roy Blunt (R-MO) introduced, the *Data Security Act of 2011 (S.1434)*, a NAFCU-backed financial services approach to the issue, which has been referred to the Senate Banking Committee for further action. Both bills would require security

standards for different types of personal and account information, and require specific notification procedures in the event of a breach.

Additionally, Senator Patrick Leahy, Chairman of the Senate Judiciary Committee, introduced the *Personal Data Privacy and Security Act of 2011*, which has been marked-up and placed on the Senate Legislative Calendar under general orders. Senator Leahy's bill would provide for enhanced punishment for identity theft and other violations of data privacy and security, require security standards for certain types of personal and account information, require certain disclosure and maintenance procedures for data brokers, and authorize the Attorney General and state attorneys general to bring civil actions against business entities for violations of the Act.

While supporting some aspects of proposed legislation, NAFCU has developed a list of items we would like to ultimately see addressed in any comprehensive data security bill:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card fraud be reduced. A reasonable and equitable way of addressing this concern would be to require merchants to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame. The entity that is best situated to mitigate the risk to sensitive data should be the liable party when a breach occurs.
- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no similar comprehensive

regulatory structure akin to GLBA that covers retailers, merchants, and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any business entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to by providing their personal information. NAFCU believes that this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant, but would provide an important benefit to the public at large.
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the timely disclosure of identities of companies whose data systems have been violated, so consumers are aware of those that place their personal information at risk.
- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and continue to store sensitive personal data in their easily breached systems.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised, personally identifiable information when associated accounts are involved.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the entity that has been breached. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information, but sustained a violation

regardless. The law is currently vague on this issue, and NAFCU therefore asks that this burden of proof be clarified in statute.

There are two motivating factors as to why those who collect and hold sensitive information do not do enough to protect it. First, the cost associated with the data breach often falls on others. Second, because others – for example a financial institution issuing the payment cards with new numbers – generally have to repair the problems caused by a data breach, consumers often incorrectly assume that these institutions were responsible for the breach. The first notification consumers often receive that their information may be compromised is often a call or letter from their credit union. By looking out for, and taking care of, their members, credit unions (and other financial institutions) can unintentionally suffer ill will from a member who finds out that their payment card from that institution has been re-issued. Thus the companies responsible for the data breach in the first place oftentimes do not suffer any loss of customer goodwill; at the same time consumer confidence in financial institutions, such as credit unions, may suffer. Furthermore, for a credit union such as AAFCU that serves a number of military members that may be deployed overseas, the impact on those members is magnified due to the longer postal time to get new cards to them.

While, the reputation risk to financial institutions may be difficult to solve with legislation, Congress should consider holding accountable those companies that are responsible for significant data breaches. There must be a strong incentive for businesses to properly protect consumer's financial data, otherwise, as evidenced by recent instances of payment card breaches,

the information may not be adequately protected and the credit union could end up being the one that pays.

Obviously, data breaches will continue to be a fact of life for any company that holds personal information. Unfortunately, no matter how quickly government and industry reacts, criminals will always find new and inventive ways around security measures. It is important that there be stiff penalties and full enforcement of the laws that prohibit and punish the actual criminals who take the action to commit these breaches by stealing, and often selling or using this compromised data. However, additional federal incentives to protect data are absolutely necessary. Any legislation that does not place the burden on responsible parties will ultimately prove toothless. Current data security standards established by payment card companies such as Visa and Mastercard prohibit storing sensitive data and even impose fines for those that do. However, either because the penalties are not harsh enough or the contracts aren't enforced, data ends up being stored improperly and breaches still end up occurring.

Finally, it should be noted that financial losses to credit unions are especially troubling, because unlike banks and other financial institutions, credit unions do not make profits for shareholders, do not issue stock, and aren't able to turn to capital markets for money to make up for data breach losses. All monies at a credit union must be raised through its members. Financial losses to the credit union are ultimately passed back to the member in the form of either reduced services, lower dividends on savings, higher interest rates on loans (either personal or business), or even decreased availability of loans.

Conclusion

In conclusion, NAFCU supports new measures to ensure industry takes adequate steps to protect consumers' sensitive financial data. The most efficient way to address the growing number of data breaches is to create a comprehensive regulatory scheme for those entities that currently have none. A safe harbor for financial institutions already in compliance with section 501 (b) of Title V of the GLBA should be included in any data security bill. Further, if more regulations are needed to address new concerns, it should be the functional regulators that are charged with promulgating new rules. Finally, merchants, retailers, data brokers or any other party that holds sensitive consumer information should be held financially accountable if it is responsible for a data breach.

Thank you again, Chairwoman Ellmers, Ranking Member Richmond, and members of the Subcommittee for the invitation to testify before you today. NAFCU appreciates the opportunity to weigh in on this important issue..

STATEMENT OF THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

DR. PHYLLIS SCHNECK, VICE PRESIDENT FOR McAfee, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

SUBCOMMITTEE ON HEALTH CARE AND TECHNOLOGY

CYBER SECURITY: PROTECTING YOUR SMALL BUSINESS

DECEMBER 1, 2011

Good afternoon Chairwoman Ellmers, Ranking Member Richmond, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer-Global Public Sector for McAfee, testifying on behalf of the Software & Information Industry Association (SIIA). We appreciate the Subcommittee's interest in cyber security as it affects small business, which plays such a large part in the nation's economy.

My testimony will focus on the following key areas:

- The national security implications of protecting small business from cyber attacks
- Today's cyber security threat landscape
- Practical steps small businesses can take to protect themselves from cyber attacks
- Policy recommendations to support the small business community and improve public/private sector information sharing that is essential to give the government the capabilities it needs to respond to the modern cyber security challenge

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

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

information analytics that has been used to prosecute over 300 cyber criminals worldwide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I have also served as a commissioner and working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Prior to joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

McAfee's Role in Cyber Security

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

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

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers, who can now snap into our extensible management platform. Today, more than 100 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

SIIA's Role in the Technology Sector

SIIA is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic content for business, education, consumers and the Internet. As leaders in the global market for software and information products and services, many SIIA members provide products and services that protect businesses, consumers and the

public sector from cyber-attacks, viruses, and a wide range of online security threats. While SIIA's members include many of the largest and well-known businesses in the technology industry, our membership is largely comprised of small and medium-sized companies that are the focus of this Committee.

The Critical Role Small Business Plays in the Nation's Cyber Security

In a recent op-ed in *The Washington Post*, Harvard Professor Jack Goldsmith refers to the Pentagon's claim that it will defend the country against large-scale cyber attacks. He observes, however, that small-scale cyber exploitations are far more common and actually pose a more serious national problem, as they are designed to copy or steal information, exploiting valuable government and business secrets. So-called small-scale incursions and are vastly more pervasive than cyber attacks, Professor Goldsmith states, and thus constitute a more serious threat to the nation's security.

Having investigated a number of cyber infractions over the past year that systematically drain companies' sensitive information, I wholeheartedly agree that often the more dangerous threat is not the high-profile, large-scale "hack" but rather the low-level incursion that sinks below the radar screen. Some of these constitute what security professionals call an Advanced Persistent Threat (APT), which I will discuss in more detail later, and the APT can affect organizations of any size. Small businesses are particularly vulnerable, as often cyber security is considered a "nice to do" rather than a "must do," sometimes because of budget constraints. Yet the intellectual property of a small business – let's say a small government contractor or an entrepreneurial start-up – can be just as critical to national security or the next technological innovation as that of a large enterprise.

The importance of small business to the national economy cannot be overstated. According to the Small Business Administration (SBA), small firms

- Represent 99.7 percent of all employer firms
- Employ about half of all private sector employees
- Pay 43 percent of the nation's private payroll
- Have generated 65 percent of new jobs over the past 17 years

Significantly, small firms also hire 43 percent of all high tech workers and produce 16.5 times more patents per employee than large patenting firms. Thus they are equally important to the country's collective intellectual property. Small businesses have a wealth of information – from both the public and private sectors – that could be quite valuable to a foreign nation or enterprise. And of course many of the country's most successful large businesses, such as Apple and Google, started out as small businesses.

It is also important to remember that small businesses are part of the U.S. infrastructure and network fabric, meaning that efforts to enhance the cyber security of small businesses contribute to the security posture of the entire nation. While small businesses have fewer resources to dedicate to cyber security, they face the same risk. And the risk is not just an IT risk but also a risk to the entire business. Thus we believe that managing a business's security ought to be the province of senior business leaders – not simply the IT department. As high-profile cases have demonstrated, cyber risks are growing in complexity and number.

Today's Cyber Security Threat Landscape

Today's cyber threats are more sophisticated and targeted than ever and are growing at an unprecedented rate, necessitating advanced protection and instantaneous remediation. McAfee Labs finds, for example, that both malicious URLs and malware have grown almost six-fold in the last two years, and that 2010 saw more new malware than all previous years combined.

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

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

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

In the past year alone, McAfee has uncovered numerous cyber exploitations, three of which drew particular attention: Operation Shady RAT, Operation Aurora and Night Dragon. Each of these qualifies as an Advanced Persistent Threat (APT).

The most recent APT operation we uncovered, in July 2011, is known as Operation Shady RAT (for "Remote Administration Tool"). Operation Shady RAT has been stealing valuable intellectual property (including government secrets, e-mail archives, legal contracts, negotiation plans for business activities, and design schematics) from more than 70 public and private sector organizations in 14 countries. The list of victims ranges from national governments to global corporations to tiny nonprofits, and includes government agencies in the United States, UK, Taiwan, South Korea and Canada. The vast majority of victims (49) were U.S.-based companies, government agencies, and nonprofits. The category most heavily targeted was defense contractors (13).

As mentioned earlier, the APT is much more dangerous than the high-profile attack because it is an insidious, persistent intruder meant to fly below the radar screen and quietly explore and steal the contents of the target network. This kind of low profile but highly targeted threat is analogous to cyber espionage as it provides ongoing access to protected institutional information. Such quiet yet dangerous intrusions are not limited in their scope. They can affect any company, government body or nation, regardless of sector, size, or geography.

The onslaught of increasingly sophisticated targeted attacks is reflected in growing information breach statistics. A 2010 survey found that 60 percent of organizations report a "chronic and recurring loss" of sensitive information. More than one million small businesses and retailers were victims of some type of information theft in 2010. Physical theft or tampering with point-of-sale terminals was experienced by 37 percent, while computer viruses and malware were seen by 22 percent. Fifty-six percent of small and mid-sized businesses experienced some type of banking-related fraud in 2010, with 75 percent of this coming from online sources, most prominently online account takeovers. Among small businesses falling prey to bank fraud, 61 percent were victimized more than once.

While small businesses fall prey to the same security risks as large businesses, they generally cannot allocate large amounts of costly and scarce resources to security and compliance. Small firms cannot afford a dedicated security staff, nor do they have million-dollar budgets to purchase enterprise security solutions. Regardless, small companies must meet the same security and compliance requirements as Fortune 500 firms to remain in business. What's more, any business that experiences a security breach must spend increasing amounts of capital on investigations, individual notifications to persons with personal information exposed, strengthened security countermeasures and programs, and, increasingly, legal fees and fines. Then there are the intangible costs to reputation, brands, and goodwill — costs that, in some cases, can exceed the tangible costs.

Small Business: Maintaining Strong Security with Reduced Budgets

The average security budget for all companies is around 5 percent of the total IT budget, with some sectors, such as financial services, spending a considerably higher percentage. In the current economic climate businesses are generally spending less on their IT budgets. Yet security requirements continue to grow. The news is not all doom and gloom, however, because small businesses are often more creative in their approach to challenges.

A classic example of how small businesses can maximize their investments and get more bang for their security and compliance buck is demonstrated in the early adoption of three new security and industry trends—Software-as-a-Service (SaaS), managed security services, and dedicated security appliances. Both cloud-based services and security appliances offer new bundles of security and compliance functionality at lower prices than previously available. While these technologies were not well understood and initially were viewed as more risky when introduced, they both require far less time and capital to be deployed than traditional enterprise software solutions.

Small businesses have a deep and fundamental appreciation of the linkage between managing business risk and competitiveness. They intuitively understood the agility and economic benefits of cloud-based software and security services. Small businesses became early and enthusiastic users, launching the growth in SaaS and managed security services while propelling growth to double digits. The economics caught the attention of large enterprises that fueled a second wave of growth.

The trend to increased use of SaaS, cloud-based managed security services and dedicated security appliances is expected to further accelerate and outpace licensed software until it becomes “the preferred purchasing method.”

Risk Management for Cost-Effective Security

Meeting tougher security requirements is not optional for any business, regardless of size. However, it is possible to have strong, effective security efficiently delivered at an acceptable cost – a fundamental requirement for small business. We recommend three guiding principles to make the cost of security most effective:

- Minimize the amount of sensitive information retained in the organization
- Practice risk management first
- Buy the appropriate level of security

I will say a little bit about the first two principles.

Minimizing the Amount of Sensitive Information

Many organizations have repositories of sensitive employee and customer data for internal use or to provide revenue-generating services, such as billing or insurance claims. Minimizing the types of sensitive information processed is not always an

option when the strategy of the business is to add value by processing finance, healthcare, or consumer information. However, where possible, efficiencies can be gained by reducing the number of locations where sensitive information is processed or stored. Consolidating systems and locations that process and store sensitive information reduces risk and the cost of protecting sensitive information in multiple locations.

A related strategy to sensitive data minimization is obfuscation. New technologies such as tokenization, or proven ones like encryption, require keys or indexes to make the information usable by humans. It can greatly reduce the cost of protecting sensitive information after consolidation. Risk is reduced because specific exemptions are allowed for breaches of encrypted information that eliminates the costly notification step.

Risk management for security and compliance

Experts across the security, compliance, and risk management spectrum agree that the most cost effective way to manage security and compliance starts with classic risk management. Compliance regulations require a periodic and documented assessment of risks to sensitive information. A risk management assessment is no longer optional for businesses covered by compliance regulations.

IT risk management brings an insurance paradigm to security and compliance. It is increasingly practiced in the public and private sectors, with a track record in producing cost savings, stronger security, and better compliance. Risk management is comprised of four phases:

- Identifying information assets
- Assessing threats and vulnerabilities
- Mitigating risk
- Monitoring and reporting

It is important to remember that security is a journey, not a destination. The security journey requires continuous monitoring of safeguards, critical systems and information, and new developments in the threat universe. It is also important for any business – particularly a small business – to choose a security partner that will help them make the most of their scarce resources.

Policy Recommendations

Very broadly, there are two schools of thought on government's role in achieving a desired outcome: one that posits that regulatory mandates are the best way to incent good behavior (in this case, strong cyber security measures); and, alternatively, one that asserts that positive outcomes are best achieved via positive incentives.

One might expect firms that make their living selling computer network security solutions to favor the former, a heavily regulatory model. Without question, a restrictive, sky-is-falling regime focused on mandates and elaborate regulation would compel organizations, across sectors, to spend lots of money on network security.

However, the heavily regulatory approach would not necessarily make organizations more secure – just more compliant. On the other hand, positive incentives have a higher probability of success in two ways: a higher chance of better actual outcomes, and a higher probability of producing legislative success. The private sector responds to incentives, and aligning the interests of the private sector with the outcomes that are in the national interest makes sense. Doing so could also provide rare proof that the phrase “win-win” is not always a cliché. Furthermore, positive incentives (rather than negative ones) are clearly the most effective way to drive higher levels of trust and actual cooperation between the private sector and government – vital things needed to produce real success.

Fortunately, we are not starting from scratch. There are a variety of approaches focused on incentives in play. The recommendations of the House Republican Cyber security Task Force are a step in the right direction, and there are a number of promising approaches in development on the Democratic side of the aisle as well. With the goal of encouraging collaboration and advancing an incentives-based approach to enhancing cyber security among small businesses, we support the following approaches:

- **Litigation/Legal Reform:** Imposing limitations on liability for damages as well as for non-economic losses would remove a serious obstacle to information security investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company’s good faith investments in adequate information security. Eliminating that risk, at least for companies that meet high, “best practices” security standards, would encourage more security on a company-by-company basis. This approach can help create positive incentives for disclosure through liability relief for responsible organizations to improve the nation’s overall cyber security posture.
- **Public/Private Partnership on Information Sharing:** To further promote public/private partnerships, several existing models can be especially helpful. For instance, the Departments of Defense and Homeland Security manages many public/private partnerships, and McAfee plays a role in several. These partnerships are examples of success that should be emulated, as they aim to ensure that senior corporate and government officials share vital information and best practices.
- **Competitions, Scholarships, and Research and Development Funding:** Cyber security competitions and challenges, as well as scholarship and creativity to

programs, can help identify and recruit talented individuals to the field to augment the future cyber security workforce. Similarly, research and development grants foster innovation and advance basic and applied solutions. Recognizing this, several legislative proposals under consideration contain provisions designed to help industry meet the cyber security challenges of tomorrow and train the next generation of experts.

- **Tax Incentives:** Accelerated depreciation or refundable tax credits are being considered to encourage critical infrastructure industries to make additional investments in cyber security technologies, solutions, and human capital. The same approaches could be effectively applied to small businesses. Despite the current environment where balancing the budget is a critical priority, we cannot afford to be shortsighted. Cybersecurity-related tax incentives would prove to be a legitimate, long-term investment in security that would protect our national security and economic interests.
- **Insurance Reforms:** Many companies defer investments in improved security out of a concern that, even with improved security, they are not protected from liability for losses that occur. Similarly, insurance carriers are reluctant to create a vigorous marketplace for cyber-security insurance, thereby hindering investment. Government should give consideration to implementing reinsurance programs to help underwrite the development of cyber security insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gained experience with cyber security coverage.

Government Attention to Small Business Cyber Security

While there is more that government could do to help small business fund effective security measures, I want to note some existing efforts that are headed in a positive direction.

McAfee is involved in the Federal Communication Commission's launch of the Small Biz Cyber Planner, an online resource to help small businesses create customized cyber security plans. This initiative represents a partnership among government agencies, industry groups, and private sector companies, and it is intended particularly for businesses that lack the resources to hire a dedicated cyber security staff. The tool will walk users through a series of questions to determine what cyber security strategies should be included in the planning guide, then create a customized cyber security template.

In addition, SIIA supports the recent effort by the Departments of Commerce and Homeland Security to create a voluntary industry code to address the detection and mitigation of botnets - malware distributed indirectly by networks of computers that have been corrupted by a criminal actor, turning the computers into elements of a robot network. We endorse the concept of a voluntary approach, in which the

government brings together relevant parties to confer on best practices to discuss how the private sector can develop and maintain timely and voluntary programs to detect and notify end-users that their machines have been infected with botnets or other malware and provide mitigation support that will eliminate these infections.

Another initiative that will benefit businesses of all size is the agreement between NIST, the Department of Education, and the newly formed National Cybersecurity Education Council to develop a strategic public-private partnership to promote formal cyber security education. This program is designed to help the National Initiative for Cybersecurity Education broaden the pool of skilled workers capable of supporting a cyber-secure nation.

Finally, collaboration and cooperation between the public and private sector are key to addressing cyber security in a holistic way. With the right industry-government collaboration, networks of the future can comprise intelligence and create resiliency by instantly rejecting harmful code in milliseconds just as our bodies reject viruses even though we may not know the name of the particular disease. Such advances – and others that I cannot even imagine right now – will be critical to protecting all sized businesses and organizations. In the best American tradition of collaboration, the public and private sectors have made important strides to address the cyber security challenge and enhance working relationships. We look forward to participating in the ongoing efforts to secure the valuable IP resources of our small businesses, large businesses and government, for as I hope I have shown through this testimony, all three are often connected.

Thank you for your interest and I will be pleased to answer any questions.



PREPARED TESTIMONY OF THE NATIONAL CYBER SECURITY ALLIANCE
MICHAEL KAISER, EXECUTIVE DIRECTOR

ON THE STATE OF CYBERSECURITY AND SMALL BUSINESS

BEFORE THE
COMMITTEE ON HOUSE SMALL BUSINESS SUBCOMMITTEE ON HEALTHCARE AND TECHNOLOGY

UNITES STATES HOUSE OF REPRESENTATIVES

WASHINGTON D. C.

DECEMBER 1, 2011



Chairwoman Ellmers, Ranking member Richmond, and members of the subcommittee, thank you for the opportunity to testify today on the current state of cybersecurity and small businesses. My name is Michael Kaiser and I am the Executive Director of the National Cyber Security Alliance (NCSA). Thank you for inviting me to discuss the current state of cybersecurity and small businesses.

Since its inception ten years ago, the issue of cybersecurity has been the core area of work for the National Cyber Security Alliance. NCSA is a 501 (C) 3 nonprofit organization. We operate as public private partnership working with industry leaders and government on education and awareness issues in cybersecurity. NCSA's Board of Directors is comprised of representatives from 18 companies: ADP, AT&T, Bank of America, Cisco, EMC², ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin, McAfee, Microsoft, PayPal, SAIC, Symantec, Verizon and VISA. In addition, NCSA works with many other companies, nonprofit organizations, government agencies and education institutions to achieve our mission.

NCSA is the leading education and awareness nonprofit on cybersecurity. NCSA leads critical efforts such as the STOP. THINK. CONNECT., the first ever national cybersecurity awareness campaign (in partnership with the Anti-phishing Working Group) and the

Department of Homeland Security as the lead Federal Partner, National Cyber Security Awareness Month, and Data Privacy Day. NCSA has a long track record in conducting surveys about the practices of individual computer users and small businesses as well as the state of cybersecurity education in U. S. schools. NCSA recently signed a memorandum of understanding with the Department of Education and National Institute of Standards and Technology to establish a public partnership to address the county's approach to cyber education from basic education to career pathways.

This past October, NCSA released the results of a study conducted in conjunction with Symantec about the cybersecurity practices of small businesses. The study was conducted by Zogby International, which polled 1,045 U.S. small business owners.

There is little doubt that small businesses are becoming increasingly dependent on the Internet and the survey bears this out. Businesses still allow a considerable amount of risky behavior and don't have employee policies in place or strategic approaches to cybersecurity. This all leads to a false sense of security on the part of small business operators.

The Internet has become a critical engine for small business. Business operators surveyed reported high integration of the Internet into their daily business:

- Two-thirds (66%) say that their business is dependent on the Internet for day-to-day operations

- two-fifths (38%) characterize it as very dependent
- two-thirds (67%) say they have become more dependent on the Internet in the last 12 months.
- Sensitive information businesses report handling:
 - more than two-thirds have customer data (69%)
 - almost half deal in financial records and reports (49%)
 - almost one-quarter (23%) have their own intellectual property
 - nearly one-fifth (18%) handle intellectual property belonging to others outside of the company.
- A majority of small business owners (57%) say that the loss of Internet access for 48 straight hours during a regular business week would be disruptive to their business and two-fifths (38%) say it would be extremely disruptive.

Small businesses have a lack of cyber security policy, planning and practice:

- seventy-seven percent (77%) do not have a formal written Internet security policy for employees.
- of those who don't have a formal policy, almost half do not have an informal policy either (49%)
- a majority (56%) do not have Internet usage policies that clarify what websites and web services employees can use

- almost two-thirds (63%) do not have policies regarding how their employees use social media.
- two in five small businesses (40%) do not have a privacy policy in place that their employees must comply with when they handle customer information
- almost half (48%) do not have a plan or strategic approach in place for keeping their business cyber secure.
- More small business owners say they do not (45%) provide Internet safety training to their employees than those that do (37%).
- Two thirds (67%) allow the use of USB devices in the workplace.
- Six in ten (59%) say they do not require any multifactor authentication for access to any of their networks
- only half (50%) say that all of their machines are completely wiped of data before disposal.

Yet, in spite of the poor practices and the lack of planning and policies and policies, cybersecurity is increasingly important to the value of a business:

- Seven in ten (69%) say that Internet security is critical to their business's success.
- A majority (57%) believes that having a strong cyber security and online safety posture is good for their company's brand.

We also found a disconnect exists between perceptions of cyber security preparedness and reality among U.S. small businesses:

- Two fifths (40%) say that if their business suffered a data breach or loss such as loss of customer or employee information, credit or debit card information or loss of intellectual property, their business does not have a contingency plan outlining procedures for responding and reporting it.
- Small business owners are most concerned about their employees picking up a computer virus while on the Internet (32%), followed by:
 - spyware/malware (17%)
 - loss of data (10%)
 - ID theft (8%)
 - loss of customer information (8%)
 - loss of intellectual property (4%)
 - seeing objectionable content and loss of employee data (1%)

Small businesses are increasingly using mobile devices, however:

- the majority (72%) do not let employees access company files/data remotely from mobile devices
- More than half (59%) work from home computers/access company information from personal mobile devices
- More than a third (37%) do not have employee policy/guidelines in place for remote use on mobile devices.

Despite all of these security risks and concerns, a very large majority (85%) say that given the measures they have taken, their company is safe from hackers, viruses, malware, and cyber-security breaches.

- Three quarters (72%) say they would know if their computer network was compromised
- nine in ten (91%) say their company has never suffered a security breach in which important information was stolen from a computer or their network.
- Of those who did suffer a breach, the majority says they told their customers about it (57%).

Small businesses need well-trained employees ready to use technology safely, securely, ethically and productively. When employers were asked to rate skills necessary for new hires, U.S. small businesses report the following skills are very relevant or essential:

- Understanding privacy (51%);
- Importance of protecting intellectual property (49%);
- Basic knowledge of using technology ethically (47%);
- Basic knowledge of Internet security practices (passwords, identifying secure websites) (44%).

The complete study can be found at:

http://www.staysafeonline.org/sites/default/files/resource_documents/2011%20SMB%20Study%20.pdf.

This data shows that we need to not only reach individual small businesses and help them build a better-defended environment, but that the entire small business ecosystem is at risk. We need to instill cybersecurity as a basic practice at all small businesses connected to the Internet. Small businesses owners need to see themselves as not only protecting themselves but also protecting their customers, their employees and the Internet. They need to understand that increasingly, cybercriminals see small businesses as targets. Cybercriminals know, as our data suggests, that small businesses are less defended and more vulnerable. And it may be easier or more profitable to steal money or data from a small business than to try and harvest millions of credit card or other records. By compromising a small business, cybercriminals can steal data, for example that of customers, and use the trusted relationship of the small business to prey on their customers, such as sending phishing emails that look like they come from the business and are sent to real customers and appear to be from a person they know.

Small businesses sense of security is especially unwarranted given that 40% of all targeted cyber attacks are directed at companies with less than 500 employees, according to Symantec data (<http://bit.ly/njTeMU>). In 2010, the average annual cost of cyber attacks to small and medium sized business was \$188,242. What's more, statistics

show that roughly 60% of small businesses will shut down within six months of a cyber attack (<http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9>). According to the Norton Cybercrime Report, the total cost of cyber crime to consumers and small business owners alike is greater than \$114 billion annually (<http://norton.com/cybercrimereport>).

Therefore, we must look at cybersecurity more broadly as an economic security issue. We can ill afford to have our small businesses under constant attack. It is difficult enough for small businesses to make it and thrive; we shouldn't be losing them to cybercriminals.

Changing the cybersecurity posture of small businesses is going to take a collaborative effort. Small businesses are difficult to reach on this issue. Generally the owner/operators in charge of IT issues (59% according to the NCSA/Symantec study) as one of the many hats they wear, and may see cybersecurity as either a cost burden (32% in the NCSA/ Symantec study reported lack of funds to invest as an obstacle) or as not critical (23% in NCSA/Symantec study report cybersecurity as just a nice thing to have). To be effective any efforts should include a broad array of stakeholders from industry, government, and nonprofits. There is no single company, government agency, trade association or nonprofit group that can take on this vast issue alone or reach every small business. Working together, leveraging each others resources and engaging networks—trade associations, government agencies, industry leaders and others—that small

businesses already trust, is our best hope for making the wide scale impact that is needed.

Based on the premise of a collaborative approach here are some specific suggestions to address the cybersecurity issues of small businesses.

- **Create a harmonized message and campaign that can be deployed by key stakeholders.** Like the STOP. THINK. CONNECT. campaign, a harmonized message used by trusted entities in the small businesses community could go a long way towards clarifying for businesses owners the need to have up-to-date cybersecurity practices and inspire them to action and take responsibility for securing their businesses. This campaign should be built around positive messages about the role of cybersecurity in growing a business and should be built by a diverse partnership of industry, government and nonprofits. The campaign should be based on research to see what messages would resonate with small businesses. Negative or fear based messages are unlikely to be effective. In a study NCSA conducted with VISA in 2010, we found that 85% of small businesses believe they are less of a cybercrime target than large companies
http://www.staysafeonline.org/sites/default/files/resource_documents/2010_NCSA_VISA_SB_Study_Factsheet_FINAL%2011%2023.pdf), which is clearly in opposition to previously stated data. In addition to creating awareness about the need for cybersecurity in small businesses the campaign should include advice

about basic protections—software updates, basic security practices (password management, authentication, etc.)—training materials for employees and best practices. By unifying the messaging across all trusted networks, we have the best chance of reaching every business and strengthening the entire small business ecosystem.

- **Align forces within the Federal government to support small businesses and cybersecurity.** As one of the most important factors in a strong economy, many federal agencies have an interest in helping small businesses grow while protecting their digital assets. By working together, Federal agencies can bring their expertise to the table and assist each other in outreach and education of small businesses. At a minimum, the Small Business Administration, The Department of Commerce (including representation from NIST), the Federal Trade Commission, the Federal Communications Commission and the Department of Homeland Security should participate. Others such as the Department of Defense and Internal Revenue Service, that work with or reach small businesses should also be included. A unified government approach would take advantage of each agency’s reach and day-to-day contact with small businesses.
- **Engage local communities in the effort.** Small business owners are perhaps most likely to be influenced by their peers at the local level. These are the people they interact with on a day-to-day basis and they may also belong to local groups— Chamber of Commerce, Rotary or other business/civic association. A few

forward thinking communities such as Washtenaw County, MI, San Diego, California, San Antonio, Texas and Colorado Springs, CO have started efforts to make their communities more cyber secure. In each community, they have prioritized helping small businesses. They recognize the important role small businesses play in their communities and the need to strengthen their community's cybersecurity must include small business if they are going to be successful. Because they are local and the leaders of these efforts are known and trusted community members, they can reach many small businesses others cannot.

- **Support education reform that leads to graduating a more cyber-capable workforce.** In the 21st century, we will need a workforce that understands how to use technology safely. We can assume, given current trends, that a vast majority of jobs will include using Internet connected technology. To be successful, small businesses will need a workforce ready, when they graduate high school and college, be educating young people to be safe and productive employees from day one. We know that in the K-12 education system children are not getting the basics of a cybersecurity education. Research NCSA conducted with Microsoft found that the topics are not being taught in the classroom, teachers do not feel prepared to teach the topics and teachers are not receiving professional development on the topics. As an example the survey found that, 76% of K-12 teachers had received less than 6 hours professional development on these topics in the last year. More than a third had received 0

hours

http://www.staysafeonline.org/sites/default/files/resource_documents/K-12%20Study%20Fact%20Sheet%20FINAL_0.pdf). In addition to basic skills of all employees, it is likely that small businesses will also increasingly need the help of trained cybersecurity experts to insure that their business are keeping up with the latest security practices, technology and threats. We face a serious shortage of trained cybersecurity professionals in this country. Right now large industry and government are competing for the graduates that do exist and estimates of the need for new professionals ranges up to more than 700,00 in the Americas and almost 2 million worldwide by 2015 (ISC2: www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf). The needs of small business aren't even considered in these the numbers. NCSA has signed an memorandum of understanding with the Department of Education and the National Institutes of Standards and Technology to lead the National Cybersecurity Education Council (NCEC), a public-private partnership, to collaborate with the National Initiative on Cybersecurity Education, led by NIST, to address cybersecurity education issues at all levels including basic cybersecurity education, the development of the professional cybersecurity workforce and workforce training. Our aim is to build a consensus around the path forward from a large and diverse stakeholder group that can also help with implementation.

- **Highlight and leverage existing resources.** There are many good resources available for small businesses on cyber security such as the U. S. Chamber of Commerce's Internet Essential for Small Business (<http://www.uschamber.com/issues/technology/internet-security-essentials-business>) and the FCC's new online small business cyber planner (<http://www.fcc.gov/cyberplanner>) to name just a couple. Industry, including software and hardware manufacturers and Internet Service Providers, have a wealth of information and resources. Getting the word out about materials that can help small businesses today is important.
- **Encourage members of congress to make information available to the small businesses in their district or to hold a cybersecurity for small business town hall.** NCSA believes that if members reached out to the private sector to provide content for the town halls that there would be many companies willing to participate in providing content.

Thank you again for the opportunity to testify on this critical issue. I look forward to your questions.



**Statement of the
Computing Technology
Industry Association
Before
House Committee on Small Business
Subcommittee on Healthcare and Technology
“Cybersecurity: Protecting Your Small Business”**

**Thursday, December 1, 2011
2360 Rayburn House Office Building**

Introduction

Chairwomen Ellmers, Ranking Member Richmond, and distinguished members of the Subcommittee, on behalf of the Computing Technology Industry Association (CompTIA), we appreciate the opportunity to submit testimony for the record. We wish to thank Chairwomen Ellmers and Members of this Subcommittee for holding this hearing on “Cybersecurity: Protecting Your Small Business.”

About CompTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association representing the \$3 trillion global information technology (IT) industry. CompTIA membership includes over 2,000 members and 1,000 business partners. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. These members include computer hardware manufacturers, software developers, technology distributors, and IT specialists that help organizations integrate and use technology products and services. As a trade association, CompTIA is also the leading global provider of IT workforce certifications. Currently there are over 1.4 million CompTIA IT certification holders worldwide, and many of those are for IT security.

CompTIA is dedicated to serving its membership by advancing industry innovation and growth through its educational programs, market research, networking events, professional certifications, and public advocacy.

Background

Small and medium size businesses are the core of the American economy. There are approximately 30 million small and medium size businesses in the United States, which represent over 99 percent of all employer firms and employ over half of all private sector employees. Many participants in the IT industry are independent small businesses that provide a variety of functions for customers they serve. A sizeable portion of anticipated work force growth will emanate from start-up and small- and medium-sized (SMB) information technology firms. The SMB sector of the IT industry accounts for about

40% of industry jobs, or more than 2 million workers, and 163,000 employer businesses that maintain a payroll.

Issues

CompTIA appreciates the opportunity to provide our perspective on public policy issues that we believe have a significant impact on the ability of SMB firms to develop and/or provision innovative cybersecurity products and services. Although there are numerous public policy issues that have an impact on the cybersecurity ecosystem we would like to highlight five issues that we find most pressing at this time.

Information Sharing Practices

CompTIA believes that information sharing between the public and private sector on existing and emerging cybersecurity threats and attacks is a critical component toward the protection of US public and private infrastructure. Providing access to sensitive security information will be of great value to SMB IT firms who otherwise may not have the resources to undertake extensive security and forensics investigations. Moreover, the liability shield provided under the proposed bill is a game changer. Most SMB firms have “Errors and Omissions” policies in the \$1M to \$2M range which is hardly sufficient to cover any major cybersecurity litigation. Thus, a shield against liability serves as an incentive for SMB firms to expand their cybersecurity product and service offerings.

CompTIA Policy Recommendation

CompTIA supports the Cyber Intelligence Sharing and Protection Act of 2011 (H.R. 3523), because it achieves these important objectives, and we are hopeful that the bill will continue to receive broad and bipartisan support.

Data Breach Notification

Among the most important issues for SMB IT firms is ensuring compliance with the patchwork of state data breach notification requirements. Currently, there are over 45 jurisdictions with state specific data breach notification requirements. Thus, there is no

uniformity amongst these rules, and in many instances they conflict. SMB IT firms are forced to navigate through individual state data breach requirements to:

- Understand what type of entity is covered by the law,
- Understand under what circumstances is a state notice requirement triggered,
- Determine what is an acceptable form of customer notice,
- Review state laws to understand possible exceptions to a particular notice requirement,
- Identify the correct parties to whom the notices must be provided, and
- Understand whether the state provides for a private right of action.

Companies must work to identify and hire employees with the requisite level of expertise needed to study and understand the patchwork of data breach laws with varying compliance obligations and penalties. For a company with 10 to 20 employees, navigating through this patchwork of laws can be an expensive, if not impossible, undertaking.

For instance, Arizona's data breach law provides no notice exception and companies must provide customer notice if an unintended party acquires or gains access to a customer's personally identifiable information. However, under an Idaho law a company must provide notice to a customer if personally identifiable "information was or is reasonably believed to have been misused." The law provides an exception to the notice requirement if "after a reasonable and prompt investigation, the [company] determines that there is not a reasonable likelihood the personal information has been or will be misused."

Thus, companies may find it easier to simply send out blanket data breach notices whenever there is a suspected or actual data breach of personally identifiable information. The problem with this approach is that over time such notices begin to lose their effectiveness after consumers get accustomed to receiving them. It is similar to political or bulk mail whereby consumers become desensitized to these notices and advertisements so that the letters and/or e-mails containing customer notices go unopened and often

disregarded. Nevertheless, these firms have to incur costs associated with such notices that may not be required because an actual data breach did not actually occur.

SMB IT firms are also exposed to expensive legal costs as they try to get an assessment of their liability across a patchwork of state legal obligations and liabilities. This patchwork of state data security and breach laws serve as a considerable barrier to entry for SMB firms in the area of cybersecurity and data protection.

CompTIA Policy Recommendation

For all the aforementioned reasons, CompTIA supports a national framework for a data breach notification law.

Research and Development

Federal funding for research and development has been the bedrock of American technological superiority. Federal research programs have spawned countless industries, including the Internet, which has kept America at the forefront of technological innovation. America's SMB IT community is well positioned to continue its leadership in the creation of new and innovative cybersecurity products and services, and the federal government has an important role toward this end.

CompTIA believes that there are two core programs that serve as key models for helping American industry maintain its role as the global leader in developing technological innovation. The Small Business Innovation Research (SBIR) Program and the Small Business Technology Transfer (STTR) Program serve as springboards for small IT firms to develop cutting-edge IT products and services. There are currently numerous departments of the US government leveraging these programs to fund SMB firms that are developing innovative cybersecurity products. For example, the company viaForensics is developing cutting edge mobile security solutions under an SBIR program. This company is a prime example of the type of American ingenuity that is rising to the top through the creation of mobile security solutions. The company is growing in leaps and bounds and is an example of the growth opportunities for SMB IT firms. Unfortunately,

SBIR and STTR are only funded through 2011, and it is unclear whether the programs will survive.

CompTIA Policy Recommendation

We would urge the Subcommittee to advocate in favor of the SBIR and STTR programs as they can play a critical role fostering SMB IT firms toward the development of new and innovative cybersecurity products and solutions.

The SBA Committee on Cybersecurity

In 2009 the Credit Card Accountability Responsibility and Disclosure Act (CARD) became law. Section 507 of CARD directed the Small Business Administration to create the SBA Committee on Cybersecurity (SBACC). This Committee was tasked with developing recommendations to address the information technology security needs of SMB's. It has been well over two years since the SBACC was created, but to date there are no recommendations forthcoming.

CompTIA Policy Recommendation

We would respectfully ask the Subcommittee Chairwomen to request a report from SBA on the status of the pending recommendations.

Basic IT Skills and Computer Sciences Educational Training

Among the greatest challenges for the cybersecurity community, including the federal government and SMB IT firms, is attracting and retaining human capital in the field of cybersecurity. Indeed, CompTIA believes that cybersecurity education and training is the foundational gap that must be closed in order to address our ongoing exposure to cyber threats, attacks, espionage and fraud. This is an especially pressing issue for SMB IT firms who may not have the resources to fund and attract the limited pool of trained and certified cybersecurity professionals. As a result, market demand for trained and certified cybersecurity professionals is extremely high providing many employment opportunities for trained professionals. There are numerous reports and surveys that are tracking this trend that we would gladly furnish upon request.

Nevertheless, workforce development in general, and cybersecurity expertise in particular, has been somewhat hamstrung by a lack of accessible training and educational opportunities, which are often costly to employers and employees. While advanced degrees are important in some cases, career and technical education are vital to the IT workforce. Industry credentials are an important tool, for example, in providing IT security and specialized cybersecurity training. Small business would benefit greatly from assistance that offsets the cost of this important continuing education.

CompTIA Policy Recommendation

Amend the Lifetime Learning Credit in order for individuals and IT solution providers to offset some of the expense of earning appropriate certifications and skills for the IT marketplace. This credit is currently only available to the employee and does not apply to the expense of earning a certification of skills, which is essential to establishing the knowledge and qualifications of a job applicant.

Amend the Business Deduction for Work-Related Education to allow individuals and IT solution providers to offset some of the expense of earning appropriate certifications and skills needed in the IT marketplace. The current deduction does not currently allow employers to deduct the cost of earning a certification of skills, which is essential to establishing the knowledge and qualifications of a job applicant.

Conclusion

Thank you again for the opportunity to provide these comments for the record. We are ready to answer any possible follow up questions and would be glad to provide any additional information that you may deem helpful.



***Recommendations of the
House Republican
Cybersecurity Task Force***



TABLE OF CONTENTS

Cybersecurity Task Force Members.....	3
Introduction – Why Cyber?	4
Our Charge.....	5
How to Approach Cyber	5
Observations.....	6
Task Force Recommendations.....	7
Issue 1: Critical Infrastructure and Incentives	7
Issue 2: Information Sharing and Public-Private Partnerships	10
Issue 3: Updating Existing Cybersecurity Laws	13
Issue 4: Legal Authorities.....	15
Other Issues and Longer Term Recommendations.....	17
Appendix.....	20

CYBERSECURITY TASK FORCE MEMBERS

Rep. Robert Aderholt (4 th AL)	Appropriations
Rep. Jason Chaffetz (3 rd UT)	Budget Judiciary Oversight and Government Reform
Rep. Mike Coffman (6 th CO)	Armed Services Natural Resources Small Business
Rep. Bob Goodlatte (6 th VA)	Agriculture Education and the Workforce Judiciary
Rep. Robert Hurt (5 th VA)	Financial Services
Rep. Bob Latta (5 th OH)	Energy and Commerce
Rep. Dan Lungren (3 rd CA)	House Administration, Chairman Homeland Security Judiciary
Rep. Michael McCaul (10 th TX)	Ethics Foreign Affairs Homeland Security Science, Space, and Technology
Rep. Tim Murphy (18 th PA)	Energy and Commerce
Rep. Steve Stivers (15 th OH)	Financial Services
Rep. Lee Terry (2 nd NE)	Energy and Commerce
Rep. Mac Thornberry (13 th TX)	Armed Services Permanent Select Committee on Intelligence

Note: Bold denotes committee designee

INTRODUCTION – WHY CYBER?

Cybersecurity is a complex set of issues involving legal, economic, and national security considerations. In the House, at least nine committees have some significant jurisdictional claim on cyber issues. In May, the White House submitted its legislative language for discussion. The Senate has attempted to construct a comprehensive cyber bill for the last two consecutive congresses.

Given the difficulties, it is reasonable to ask why the House should devote time and energy to an issue that is not at the top of the public's expressed priorities. There are at least three reasons:

- 1) **Cyber is a major national security issue.** Top government, intelligence, and military leaders often point to cyber as the issue that worries them the most – partly because it touches every aspect of American life (and of military operations) and partly because our laws and policies clearly have not kept up with the rapid changes in technology. Earlier this year, CIA Director Leon Panetta testified about his fear of a “cyber Pearl Harbor.”
- 2) **The threat is real and immediate.** Essentially, every week there are news reports of some company or organization that has had data stolen – from the Department of Defense to, increasingly, small businesses. Most incidents, of course, are never made public. The potential damage, as we will discuss, involves far more than stolen or damaged data.
- 3) **Cyber is connected to our economy and job creation.** It is not just national security information that is being stolen from databases in the U.S. All kinds of intellectual property are targeted. Information stolen from U.S. databases equals jobs stolen from the U.S. economy. There are many stories of a small business developing a new product, being hacked, and finding copies of its new product flooding the market at cut-rate prices from China within a few months. We must take steps to protect American ideas.

OUR CHARGE

On June 24, 2011, House Republican Leadership formed the House Republican Cybersecurity Task Force. The Task Force was asked to make recommendations to Leadership on how House Republicans should approach four issue areas within cybersecurity:

- 1) Critical Infrastructure and Incentives
- 2) Information Sharing and Public-Private Partnerships
- 3) Updating Existing Cybersecurity Laws
- 4) Legal Authorities

HOW TO APPROACH CYBER

Based on the charge given to this Task Force, we are recommending a general framework to use in dealing with the four areas we were assigned. Our hope is that this framework can help guide House action for the remainder of this Congress and beyond.

In each of the four areas, we have offered recommendations for the near term that can reasonably be acted upon during this Congress. We have also listed other issues that could be considered or at least advanced. At a minimum, committees should hold hearings on these other issues as they are often no less serious or pressing. Solutions on a portion of those topics may be harder to identify within limited time and resources.

We believe that the current standing committees are in the best position to write the legislation that is consistent with this framework – and even more than with most issues, getting the details exactly right here is very important. Therefore, we assume that the committees will mark-up cyber bills within their jurisdiction, using regular order with active participation by all Members.

At the same time, it has been very helpful for us to have a variety of perspectives brought to the table when discussing this issue. Each of the nine committee representatives and the committees' staffs support these recommendations. But even the limited recommendations we suggest for this Congress will require continuing cooperation among committees.

Legislative packaging and vehicles must, of course, be decided by Leadership, but we are generally skeptical of large, "comprehensive" bills on complex topics, at least as the bills are being written. Individual bills could, of course, be packaged together at some point later in the legislative process.

With the current fiscally constrained environment, any new or expanded programs and initiatives need to reflect fiscal realities. We must keep in mind the potential fiscal impact on both the public and private sectors.

OBSERVATIONS

1. The country is very dependent on computer networks and information infrastructure, and that dependency is growing.
2. The advantage lies with the attacker, and that advantage is growing.
3. Currently, we are very vulnerable to a variety of attacks and exploitations from a variety of actors across the entire spectrum of sophistication.
4. We face a wide range of threats – from vandalism and petty crime to, potentially, cyber warfare and cyber terrorism, but we may not be able to tell which it is at the moment of attack.
5. Most attacks and exploitations can be stopped with ‘good hygiene.’
6. Using ‘good hygiene’ reduces the clutter that more sophisticated actors use to mask their attacks, enabling government and industry to put an increased focus on the more advanced and dangerous threats.
7. Government insights and capabilities, often derived from intelligence collection, can significantly augment the private sector’s efforts to defend against more sophisticated threats, which are often, but not always, from state actors.
8. Many malicious cyber attacks are based on U.S. servers because of the legal protection given entities in the U.S.
9. The Stuxnet computer worm represents a new, more sophisticated and more dangerous level of threat. It does more than steal or destroy data. It alters the control systems that affect physical things, like machinery.
10. Threats change and adapt rapidly. Change occurs so fast in this area that attempts to directly regulate a specific cybersecurity solution will be outdated by the time it is written.
11. Most infrastructure is owned by the private sector, and it has a responsibility to protect its networks. Government should also improve its own network security. However, government information can augment the private sector’s efforts to defend its own networks, and private sector knowledge and information can significantly assist the defense of the government’s networks.
12. There is a cultural challenge of trust and ownership involved in sharing information among government agencies and among private companies. That is even more true when it comes to sharing between government and industry.

TASK FORCE RECOMMENDATIONS

ISSUE 1: CRITICAL INFRASTRUCTURE AND INCENTIVES

Critical infrastructures are certain physical assets, functions, and systems that facilitate the production and distribution of our nation's goods and services that we depend on every day, such as power distribution, water supply, and telecommunications. The Department of Homeland Security (DHS) has divided our nation's critical infrastructures and key resources into 18 sectors.

As computer technology has advanced, so has the dependence on computerized industrial control systems to monitor and control equipment that supports modern critical infrastructures. Malicious code that alters these control systems has the potential to inflict serious – even lethal – damage.

Yet, we have been told that the free market alone may not be able to improve security sufficiently. The return on investment may be hard to prove, and businesses will only do what makes sense for the bottom line. We are generally skeptical of direct regulation and of government agencies grading the security of a private company, which is another form of regulation. Threats and practices change so quickly that government-imposed standards cannot keep up. Regulations can add to costs that ultimately come out of consumers' pockets.

Voluntary Incentives

We believe Congress should adopt a menu of voluntary incentives to encourage private companies to improve cybersecurity. Some incentives may have a cost and would have to be offset. Others do not. However, incentives should be largely voluntary, recognizing that most critical infrastructures are privately owned. Many of these incentives could also be utilized by companies that do not own critical infrastructures.

We also have to recognize that different companies and sectors will need different incentives – one size does not fit all. Committees should evaluate incentives that will be effective within their jurisdiction.

Among the incentives for committees to consider are:

- **Standards Tied to Incentives:** Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies, such as the National Institute of Standards and Technology (NIST), to help the private sector improve security. These standards should be developed by a public-private partnership, focus on security best practices, and remain technology-neutral as much as possible. Additionally, the public-private partnership should evaluate which incentives or strategies would increase the adoption of successful security best

practices. An example would include varying degrees of liability protections afforded to companies that voluntarily implement the enhanced security practices.

- **Streamline Information Security Regulations:** Many private sector corporations are subject to more than one regulator for the protection of their data. For example, Sarbanes-Oxley requires companies to certify that their financial systems are appropriately controlled; HIPAA requires control of any personal information regarding health care, similar to the requirement that the Gramm-Leach-Bliley (GLB) Act puts on personal financial information. Congress could require the Administration to coordinate with critical infrastructure sectors to develop strong performance standards that, if a company was found compliant with the new standard, would satisfy the information security/privacy protections of SOX, HIPAA, GLB etc. A company would be encouraged to implement stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators.
- **Existing Tax Credits:** To encourage companies to increase their investment in network security, Congress should consider expanding or extending existing tax credits, such as the R&D tax credit, to apply to cyber investments as an alternative to creating new tax credits.
- **Existing Grant Funding:** Existing grant funding should be evaluated as an alternative to new funds. Congress could also evaluate including minimum cybersecurity protection standards in grant proposals for grantees dealing with issues such as national security, law enforcement, and critical infrastructures as a condition for receiving government funds. These would include general protection standards such as updating computer patches or running anti-virus software that would not be overly burdensome to grant recipients.
- **Insurance:** Congress should study whether the insurance industry can help play a role in increasing the level of cybersecurity of firms that purchase cyber or data breach insurance and whether the cybersecurity insurance market is currently structured in a manner to accomplish that goal.

Targeted and Limited Regulation

There may be instances where additional direct regulation of an industry that is already highly regulated (nuclear power, electricity, chemical plants, water treatment) may be warranted. **Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity at these facilities using existing regulators.** Any additional regulation should consider the burden on the private sector by requiring agencies to conduct a thorough cost/benefit analysis.

- **Defining Critical Infrastructure:** Nearly every organization is susceptible to a cyber attack. However, it is cost prohibitive to protect everything, and not every asset, even those within critical infrastructures, will have an impact on national security or critical functions. The government should work closely with each sector to identify elements of critical infrastructure that, if damaged or destroyed, could cause great loss of life or significant economic damage impacting our national security. Further, any targeted or limited regulation should only apply to critical functions or facilities rather than entire organizations to ensure that the impact is not overly broad.
- **Private Industry Input:** Industries with identified critical infrastructures should have full and complete participation in the development of cybersecurity standards and best practices. Any standards should be performance-based rather than technology-based to ensure that they are not out-paced by the advancement of technology. Owners and operators know best how to protect their own systems, and it is nearly impossible for the speed of bureaucracy to keep pace with ever changing threats.
- **Liability Protections:** If existing regulators are imposing a jointly developed cybersecurity standard, the company should be granted some level of liability protection for following this standard. To encourage compliance, regulated entities would be granted limited liability protection in the instance of a breach if they meet or exceed mandated standards. Compliance would be determined through oversight of existing regulators.
- **Oversight:** Entities that currently regulate an element of critical infrastructure that has been defined as higher risk should be responsible for oversight. Enforcement of these standards should be incorporated into already established safety or security reviews. Any element of critical infrastructure that has processes or technology that exceed the established standard should be deemed compliant with the standard. The Department of Homeland Security should work with other regulators to help coordinate security standards across sectors and within sectors subject to multiple regulators.
- **Cybersecurity Reporting Requirements:** Congress should investigate the possibility that significant cyber incidents and vulnerabilities could be included in existing mandatory reporting to improve both law enforcement response and protection of critical infrastructure.

 ISSUE 2: INFORMATION SHARING AND PUBLIC-PRIVATE PARTNERSHIPS

Private sector entities control the vast majority of information networks and assets vulnerable to a cyber attack. Consequently, such entities are often in the best position to identify and defend against cyber-related threats. Owners and operators are, and should be, responsible for the protection, response, and recovery of private assets. The government is also responsible for its own assets.

There is widespread agreement that greater sharing of information is needed within industries, among industries, and between government and industry in order to improve cybersecurity and to prevent and respond to rapidly changing threats. For example, through intelligence collection, the federal government has insights and capabilities that many times are classified but would be useful to help defend private companies from cybersecurity attacks.

There are several organizations designed to help facilitate information sharing now, and there is some sharing going on with varying degrees of success. But not nearly enough.

We largely agree with those who believe that a new entity – separate from the federal government but perhaps partially funded by the federal government – is needed to sponsor this sharing to allow for active defense. But whether a new entity is created or an effort is made to invigorate existing structures, changes to the law are required to allow government and industry to share.

Improving Information Sharing and Developing Active Defense Capability

Companies, including Internet Service Providers (ISPs) and security and software vendors, are already conducting active operations to mitigate cybersecurity attacks. However, these are largely done independently according to their individual business interests and priorities.

Congress should facilitate an organization outside of government to act as a clearing house of information and intelligence sharing between the government and critical infrastructure to improve security and disseminate real-time information designed to help target and defeat malicious cyber activity.

- The purpose of this entity is not to replace or preclude the enhancement of existing sharing structures, but to expand information sharing to detect and mitigate cyber attacks in real time before they reach their target. Many current efforts provide threat and vulnerability information sharing after the attack has occurred. While this information is still very valuable and, in fact, will help mitigate future attacks, the main focus of this privately led facility is to provide real time defense at network speed.
- This entity would operate outside of government. There is substantial and understandable concern with the government monitoring private networks. This entity would provide a place for the federal government to plug in its knowledge of classified threat signatures and combine this information with the knowledge of threats from across the private sector. ISPs and other large network enterprises could use this

collectively gathered information to block attacks before they reach their target. Information collected by the center would need to have sensitive personally identifiable information from Americans removed and sanitized before it could be shared back to the government. It should be clear to all participants how information will be shared and for what purpose. The entity should also employ a privacy board to periodically audit information transmitted to the government to ensure that privacy standards are consistently upheld.

- We have been encouraged with the model of the Defense Industrial Base (DIB) pilot program where DIB companies, ISPs, and the government share information, including classified information, with one another to improve operational security among the participants, much like the model described above. This new entity should utilize lessons from this successful sharing of specific and actionable classified information.
- In order to utilize private sector and government information, this new active defense entity should coordinate with existing information sharing structures such as the Information Sharing and Analysis Centers (ISACs), the National Cybersecurity and Communications Integration Center (NCCIC), the Information Sharing Environment (ISE), and the United States Computer Emergency Readiness Team (US-CERT).
- For this entity to operate effectively, Congress must amend certain laws and provide narrowly targeted exceptions to allow carriers to share cybersecurity related information in order to protect themselves, their customers, and the government. An antitrust exemption might also be required.
- For those private sector entities that voluntarily participate in this new entity, Congress should provide some level of liability protection from lawsuits that result from an action to address malicious activity based upon information received as a member of the entity. Participation in the active defense entity would also limit participant liability in the case of a penetration of their system that resulted in a financial loss they reported in their required financial statements.

Legal Protections for Sharing Information

Liability concerns have also been a common roadblock for information sharing within existing structures. **We believe that information sharing within existing structures can be improved through limited safe harbors when private sector entities voluntarily disclose threat, vulnerability, or incident information to the federal government or ask for advice or assistance to help increase protections on their own systems.** These protections would need to address concerns about antitrust issues, liability, an exemption from the Freedom of Information Act (FOIA), protection from public disclosure, protection from regulatory use by government, and whether or not a private entity is operating as an agent of the government. However, the protection of personal privacy should be at the forefront of any limited legal protection proposal.

Awareness Campaign

Some estimate that 85% of the threat to our information networks can be eliminated with proper cybersecurity hygiene. Increasing the awareness of individual users will help them to protect their own information as well as to reduce the number of access points cyber criminals can use to gain access to businesses.

The first step is to educate Members of Congress. In addition to having a better understanding of the urgency of this issue, Members need to be equipped to help educate businesses and individuals within their districts. Members could also be involved in public service announcements (PSAs) about cybersecurity and good computer hygiene.

Stopthinkconnect.com is a cyber awareness campaign developed with the help of numerous private corporations, the Department of Homeland Security, and other agencies. The government should explore ways to promote cybersecurity hygiene awareness as well as support state and local efforts, through television, the Internet, and printed publications. The government should leverage the messaging talents of the Ad Council and private-sector businesses and target different age groups with similar but segmented messages on cybersecurity risks, consequences, and best practices.

Congress should also work with federal agencies to create a feedback process for this awareness campaign to measure its overall effectiveness (leveraging expertise from other government agencies, like the Broadcasting Board of Governors, Radio Free Europe/Radio Liberty, or the Undersecretary of Defense for Policy, which all have experience with this type of program assessment).

Data Breach

For many companies, the normal operation of business requires the collection and use of sensitive personally identifiable information. When this information is stolen, individuals are exposed to theft and identity loss. This threat is even greater when individuals are unaware their information has been compromised. Nearly every state has implemented its own data breach law that, at times, can make it difficult for businesses to be in compliance. Congress should address data breach notification legislation that simplifies compliance for businesses and protects the sensitive personally identifiable information of individuals.

ISSUE 3: UPDATING EXISTING CYBERSECURITY LAWS

A host of laws have not been updated to reflect changes in technology. A serious effort should be made to do so. Some updates are necessary to make progress in cybersecurity. Others are needed just to make the law relevant to today's environment. Some will be more controversial than others.

The Cybersecurity Review conducted by the Obama White House in early 2009 identified a number of laws that are in need of an update. The May 2011 White House proposal suggests updates to laws related to law enforcement and federal information sharing as well as criminal penalties and the location of data centers. Portions of these provisions are consistent with our recommendations.

Attached as an appendix are some of the laws that have been suggested to us that should be examined with an eye toward reforms. The most essential laws in need of updating in order to defend the country include:

Federal Information Security Management Act (FISMA) of 2002

FISMA is the main law governing the federal government's information security program. It requires agencies to develop and implement appropriate information security protections according to the risk and degree of harm from unauthorized access.

What needs to change? A main concern with FISMA is that it is inefficient and unable to result in adequate cybersecurity protections. Many believe FISMA has turned into a checklist exercise with a focus on procedure and reporting rather than implementing the best protections. Multiple agencies have been found FISMA compliant even though their security was extremely poor in reality.

Recommendation: FISMA needs to be reformed to focus on secure, continuous, automated monitoring of IT systems rather than the current checklist exercise, which is ineffective. Any update should enable the government to secure its systems now and in the future. Changes in technology, such as cloud or distributed computing, should be contemplated in any update/reform. The federal government needs to lead by example and ensure its own computers and networks are secure. The authorities given to the Department of Homeland Security in two Office of Management and Budget memos, M-10-15 and M-10-28, should be supported and resourced appropriately. This effort of bringing FISMA up to technological date will require multiple committees to work together on appropriate language.

Computer Fraud and Abuse Act (CFAA) of 1986

CFAA governs the unauthorized access to computers used by the federal government, financial institutions, or those used for interstate commerce. The purpose of the act is to reduce hacking of federal and certain other computer systems and includes criminal penalties for violations of the law.

What needs to change? The current definition of protected computers is narrow and applies mainly to those used by the federal government and financial institutions. Federal courts have interpreted the CFAA to include critical infrastructure, but it is not explicitly specified in the statute. Additionally, some courts have interpreted the definitions of “access” and “authorization” in different ways to apply liability without hacking.

Recommendation: The definition of protected computers should be extended to cover critical infrastructures with attached criminal penalties. This definition could also be expanded to cover all private sector computers with differing criminal penalties. The CFAA could also criminalize the creation and distribution of malware. However, while increasing the penalties associated with activities that disrupt or damage protected computers, the CFAA should also be narrowly focused to avoid unintended liability beyond computer hacking.

Communication Laws

There are current laws in place governing the protection of electronic communications that contain certain exemptions for specific activities. Many organizations, including privacy groups, recognize the need for additional and specific flexibility within these laws to allow carriers to share appropriate cybersecurity related information, to protect themselves, their customers, and the government. In addition, some sort of anonymous reporting mechanism should be developed in order to facilitate a better evaluation of risk for the development of a functioning cyber insurance market. The clearing house described above could act as the repository to assuage privacy concerns. The reporting could be similar to the public health model where the Centers for Disease Control requires the reporting of infectious diseases without sacrificing privacy and corporate concerns.

Criminal Statutes

Congress should review the criminal statutes to ensure that law enforcement has adequate tools, including training in detection and mitigation, to investigate cyber crimes. The federal government should also increase cooperation with local and state prosecutors and judges to enhance the familiarity with appropriate evidentiary regimes for securing and using computer-based evidence in prosecutions. Congress should also change the Racketeer Influenced and Corrupt Organizations (RICO) law to include computer fraud within the definition of racketeering; provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information; expand penalties for conspiracies to commit computer fraud and extortion attempts involving threats to access computers without authorization; provide for forfeiture of property used to commit computer fraud; and require restitution for victims of identity theft and computer fraud. Additionally, Congress should conduct a comprehensive examination of crimes involving computers to ensure that penalties are appropriate when compared to similar crimes committed “in person.”

ISSUE 4: LEGAL AUTHORITIES

Cyber challenges our underlying assumptions about warfare and conflict, about jurisdiction and responsibility for dealing with illegal acts, and about the relationship and interaction between government and the private sector.

Updating the legal authorities for our country to act to protect itself is among the most complex issues related to cyber. It is not at all clear what the government's responsibility is, if any, to protect a private business from cyber attack – even if the attacker is believed to be a foreign state. Increasingly, attacks are launched from servers inside the United States because of our relatively strict laws protecting private entities and because of the cumbersome process which government must use to take action against such servers. There are a number of questions that need to be addressed in this area:

1. What is the responsibility and/or authority of the federal government to defend a private business when it is attacked in cyberspace?
 - What if it is a foreign state attacking the business?
 - What if we do not know the source and what level of confidence do we need in attribution in order to take action?
2. How should we use the full range of instruments of national power and influence to discourage bad actors in cyberspace?
 - How do we develop and apply concepts of deterrence?
3. The Intelligence Community collects much information on cyber threats.
 - How do we decide which information to use to defend?
 - How do we share information at network speed?
 - How do we incorporate open source or proprietary information along with classified information to protect our networks?
4. What should the military's role be in relation to other agencies of the federal government- do the military's authorities match up with its role?
5. Apart from when the military is acting pursuant to a congressionally authorized use of force, do sufficient authorities exist to allow for offensive cyber operations necessary to protect our national security?

These are difficult questions. But it is the responsibility of Congress to pursue answers so that the nation can be protected. However, there are some areas where Congress can begin to pursue action with legal authorities.

Classified Security Networks, Information, and Role of Military

The federal government should better define a proactive process for Defense Support of Civil Authorities (DSCA) as they relate to cyber. The Department of Defense can also provide increased support to the broader federal government (as well as state, local, and tribal entities) through better leveraging of technology transition mechanisms and training opportunities.

Civilian Agency and Critical Infrastructure Networks

The federal government should continue to work to secure its own networks ensuring its data is safe and resourced efficiently. As a start, Congress should formalize the Department of Homeland Security's current role in coordinating cybersecurity for federal civilian agencies' computers and networks. As discussed above, Congress should also update the Federal Information Security Management Act (FISMA).

OTHER ISSUES AND LONGER TERM RECOMMENDATIONS

There are many issues that do not necessarily fit within one of the four areas the Task Force was asked to address. Some of them require more time for study. We believe committees should continue to evaluate and advance these issues.

Workforce Development

As we continue to work to increase our cybersecurity protections, the federal government and the private sector alike will have an increasing demand for effective skilled cybersecurity professionals. We should continue to advance educational and awareness initiatives to help meet this demand for the federal workforce, which, in turn, will benefit the private sector as well. Advancing this goal is a good step towards increasing our national security.

Recruitment, Retention, and Training

Congress should also reform the way cybersecurity personnel are recruited, hired, and trained to ensure the federal government has the talent necessary to lead the national cybersecurity effort and protect its own networks. The federal government could do more to leverage institutions designated as National Centers of Academic Excellence in Information Assurance (IA) Education by the National Security Agency and the Department of Homeland Security, including providing expedited hiring authority to graduates of these programs.

The federal government could also provide more guidance to the Centers of Academic Excellence in Research on research needs for the various federal agencies (especially those federal agencies that don't have dedicated research budgets). Congress could also consider emphasizing cybersecurity issues—detection, mitigation, resilience and rehabilitation—as priorities for development of a cadre within the National Defense Executive Reserve. The Task Force also supports revitalizing the Department of Defense's IT Exchange Program (ITEP) and granting the Department of Homeland Security additional hiring and compensation authorities similar to the White House proposal.

Federal Research and Development

Along with private sector innovation, the federal government should continue to look for ways to utilize, leverage, and coordinate its research resources and capabilities to further develop cybersecurity protections. Many departments and agencies, such as the Department of Defense, Department of Energy, Department of Homeland Security, National Science Foundation, National Institute of Standards and Technology and the Defense Advanced Research Projects Agency, can assist with this effort. The government should also have a coordinated plan to ensure that it is not duplicating industry efforts but instead making a unique contribution to safer computing.

International Cooperation and Coordination

Our world has become increasingly interconnected with consumers, businesses, and governments operating in cyberspace. Unfortunately, digital globalization has also increased our risks and made it more difficult to identify and mitigate threats between countries with different laws and different protections. For example, a bad actor can create botnets by using a computer in one country to compromise several computers in another country to carry out malicious activity often in a third country. If the host country refuses to address the bad actor, it makes it difficult for the other country to mitigate the threat of botnets.

Many perpetrators are untraceable, outside the country, or cannot be extradited. Cyber attacks are a borderless activity. The U.S. must take the lead in developing international and universal legal instruments for the prevention and punishment of nefarious cyber activity, similar to the instruments in use against terrorism and narcotics trafficking. Developing international "norms of behavior" should be encouraged.

We should also work through international development organizations to ensure that legal systems in developing countries recognize that cyber crime originating in or occurring within their jurisdiction is a serious crime with international implications, and that their legal systems move toward international standards of treatment and prosecution of such crimes. The U.S. at all levels should continue to stay actively engaged with the international community to address global cybersecurity threats.

The Task Force is also encouraged by the recent actions taken by the U.S. and Australia in adding cyber warfare to our joint defense treaty. The Administration should evaluate adding cyber to all joint defense treaties to reflect the future nature of conflicts. The U.S. should also look at foreign models for cyber defense to determine if there are lessons that might be applied to our own efforts.

Internet Service Provider (ISP) Code of Conduct

Some countries have developed certain codes of conduct that provide best practices for ISPs to apply consistently to their customers to enhance cybersecurity protections. For example, Australia has developed "icode," a voluntary code of practice, where the country's ISPs voluntarily agree to notify customers if they have compromised computers and inform users what to do about them. The Task Force encourages the U.S. ISPs to work together to develop an industry-wide voluntary code.

Supply Chain

The increasing vulnerability of the international IT supply chain suggests a legitimate need for enhanced security standards. Any approach must involve international cooperation and heavy engagement with the private sector but should not include language that might put the government in a position to determine the future design and development of technology. Congress should also investigate, perhaps through hearings, whether aspects of the 'Trusted Foundry' approach, or similar approaches, could promote innovation and help ensure domestic production capabilities for some key components.

Much like the law enforcement provisions, the U.S. must work with other governments to establish international security standards in order to prevent hobbling U.S. industry with U.S.-only standards. We are concerned about the impact on U.S. global competitiveness as well as technology innovation and development of having the U.S. government set specific technical standards.

Federal Procurement

The Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulations (DFAR) should be amended to require appropriate security technology, processes, and performance measurement in all government IT procurements. The government should use its buying leverage to create a growing market for higher security. Security technology to be included, as a matter of course, in all government procurements must be developed in conjunction with the private sector to ensure appropriate development of the regulations so that requirements do not limit the ability to use future technology.

APPENDIX

Other Cybersecurity Laws to Consider Updating**Cyber Security Research and Development Act, 2002****National Institute of Standards and Technology Act**

- The Science, Space, and Technology Committee has reported H.R. 2096 updating these two laws as they relate to cybersecurity.

High Performance Computing Act of 1991**Federal Power Act****Posse Comitatus Act of 1879****The Communications Act of 1934****State Department Basic Authorities Act of 1968****Federal Advisory Committee Act****The Privacy Act of 1974****Communications Decency Act of 1996****Identity Theft Assumption Deterrence Act of 1998****Identity Theft Penalty Enhancement Act of 2004****The Homeland Security Act of 2002****Terrorism Risk Insurance Act of 2002, as amended****Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA)****Economic Espionage Act of 1996**

SAM GRAVES, MISSOURI
CHAIRMAN

NYDIA M. VELAZQUEZ, NEW YORK
RANKING MEMBER

Congress of the United States
U.S. House of Representatives
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515-6515

House Committee on Small Business
Subcommittee on Healthcare and Technology
"Cyber Security: Protecting Your Small Business"
Thursday, December 1, 2011 1:00pm
2360 Rayburn House Office Building

Witness List

Panel 1

The Hon. William M. "Mac" Thornberry
U.S. House of Representatives (TX-13)
Washington, DC

Panel 2

Mr. David Beam
Senior Vice President
North Carolina Electric Membership Corporation
Raleigh, NC
*Testifying on behalf of the National Rural Electric Cooperative Association

Mr. Glenn Strebe
Chief Executive Officer
Air Academy Federal Credit Union
Colorado Springs, CO
*Testifying on behalf of the National Association of Federal Credit Unions

Dr. Phyllis A. Schneck
Chief Technology Officer Public Sector
McAfee, Inc.
Reston, VA
*Testifying on behalf of the Software & Information Industry Association

Mr. Michael Kaiser
Executive Director
National Cyber Security Alliance
Washington, DC

