S. Hrg. 113–790

CYBER SECURITY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

STRENGTHENING PUBLIC–PRIVATE PARTNERSHIPS TO REDUCE CYBER RISKS TO OUR NATION'S CRITICAL INFRASTRUCTURE, MARCH 26, 2014

DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM, APRIL 2, 2014

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

CYBER SECURITY

S. Hrg. 113–790

CYBER SECURITY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

STRENGTHENING PUBLIC–PRIVATE PARTNERSHIPS TO REDUCE CYBER RISKS TO OUR NATION'S CRITICAL INFRASTRUCTURE, MARCH 26, 2014

DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM, APRIL 2, 2014

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

89–521 PDF WASHINGTON : 2016

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

GABRIELLE A. BATKIN, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
MARY BETH SCHULTZ, *Chief Counsel for Homeland Security*
STEPHEN R. VIÑA, *Deputy Counsel for Homeland Security*
MATTHEW R. GROTE, *Senior Professional Staff Member*
AMANDA SLATER, *Legislative Assistant, Office of Senator Carper*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
ANDREW C. DOCKHAM, *Minority Chief Counsel*
DANIEL P. LIPS, *Minority Director of Homeland Security*
WILLIAM H.W. MCKENNA, *Minority Investigative Counsel*
JUSTIN ROOD, *Minority Director of Investigations*
CORY P. WILSON, *U.S. Secret Service Detailee*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, MARCH 26, 2014

ALPHABETICAL LIST OF WITNESSES

Page

APPENDIX

WEDNESDAY, APRIL 2, 2014

ALPHABETICAL LIST OF WITNESSES

APPENDIX

STRENGTHENING PUBLIC–PRIVATE PARTNERSHIPS TO REDUCE CYBER RISKS TO OUR NATION'S CRITICAL INFRASTRUCTURE

WEDNESDAY, MARCH 26, 2014

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Coburn, McCain, and Johnson.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. This hearing will come to order. Welcome, everyone.

This is a day that I would describe for us here in the Senate, I suspect for Dr. Coburn and me as well, it is like fitting a size 13 foot into a size 10 shoe, how we are going to make all this work. We just had a bunch of votes added this morning and this afternoon, and somehow we are going to do our best to get everything done. But thank you very much for joining us. This is an important hearing, and we are delighted that you have come.

A little more than a year ago, President Obama signed an Executive Order (EO) which put into place a number of efforts intended to enhance our Nation's cybersecurity, and we are here today to see what kind of progress has been made in implementing the Order and to gather other ideas about better securing our critical infrastructure from cyber attacks.

Every day, sophisticated criminals, hackers, and even nation states are probing our government agencies, universities, major retailers, and critical infrastructure, and they are looking for weak spots in our defenses. They want to exploit these weaknesses to cause disruptions, steal our personal information and trade secrets, or even worse, to cause us physical harm.

While we have been able to hold off some of these cyber attacks, anyone who has examined this issue even casually will tell you that our adversaries are getting into our systems every day. Earlier this week, for instance, the Washington Post reported that Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked.

One of the most significant accomplishments over the last year though, was the release of a voluntary Cybersecurity Framework.

This framework provides those who choose to implement it—whether they be government entities, utilities, or businesses large and small—with a common but flexible set of best practices and standards they can use to better secure their systems. I tend to think of the framework as a "blueprint" or "road map" to lead us toward stronger cybersecurity.

The President's Executive Order called on the National Institute of Standards Technology (NIST) including Ms. Dodson here today, to work hand-in-hand with industry to develop the framework. It is a living document, dynamic, so NIST, working with industry, will continue to update the framework to include lessons learned and to address the latest cyber threats.

From what I understand, the development of the framework ran very smoothly, and the end result is a product that has been well received by many stakeholders, some who were quite critical of our efforts in these venues previously.

In fact, just last week in Delaware, I sat down with a group of cybersecurity experts at DuPont Company who were all extremely appreciative of the public-private collaboration that went into the development of the framework. To NIST and all the partners that have worked on this framework together, I just want to say "Bravo Zulu." But I think that we can all agree that we have not yet crossed the finish line. This is not the finish line.

Right now, many organizations across our Nation are actively analyzing the framework to determine how they can use it and incorporate it into their own cyber practices. I commend those efforts, and I am pleased that we have several witnesses with us today who will share their thoughts on using the framework.

Naturally, not every company or State is ready to use the framework. Some may not even really understand what it is all about. To those organizations, I can say that help is around the corner. If you want it, we are there to help.

Under the leadership of the very talented Dr. Phyllis Schneck, the Department of Homeland Security (DHS) has launched a new voluntary program to assist organizations in adopting the framework. This program will be incredibly important to the success of the framework, and we will be closely monitoring its progress to ensure it is providing the right tools and information to stakeholders. For instance, we need to make sure our Nation's small and medium-sized businesses are getting the attention that they need to really drill down on the framework.

At the end of the day, though, I think the question that we are all asking is whether or not the framework will help improve our Nation's cybersecurity. While it might be too early to answer that key question, I do believe that the framework itself provides a much needed road map for companies that want to improve their cybersecurity, and this is a very good first step.

Of course, the framework will only be successful if companies actually use it, so it is time for industry to roll up their sleeves and put this roadmap to use to help us make it better. It makes business sense, too. In the words of Dr. Pat Gallagher, whom I think Donna knows pretty well, the head of NIST and now the Acting Deputy Secretary of Commerce, who sat right here, Donna, where you are sitting today, and said, "good cybersecurity is good busi-

ness." When those two become synonymous, we know we have gotten to a very good place.

When you consider the threats that we are up against, however, I think we can all agree that there is much more that needs to be done, and that is why we continue to believe that bipartisan legislation is the best long-term solution to address this growing concern. We have been working hard with our Ranking Member, Dr. Coburn, and our staffs, the folks at DHS, and others in an attempt to produce such legislation.

For example, I think we need to modernize the way we protect our Federal networks from cyber attacks. There is not much argument about that.

We also need to clarify and strengthen the public-private partnership that we want the Department of Homeland Security and industry to have regarding cybersecurity.

And we need to make information sharing easier so that companies can freely share best practices and threat information with each other and with the Federal Government. And, finally, we need to continue to develop the next generation of cyber professionals and enhance our cyber research and development efforts right here at home.

Last week, I had the privilege of visiting a new cybersecurity class and program at the University of Delaware. I was very impressed with the students and was even told—they were from not only all over Delaware but all over the country and from around the world. But I was told that the class was "oversubscribed to both," undergraduate and graduate students. I think that is a good problem to have.

The students at the University of Delaware, they get it. They understand what cybersecurity means and how important it is for our economic and national security. Our friends with us today understand it, too. But for some other folks, this is just a hard issue to grasp.

It is my hope that the framework can help us jumpstart a new conversation about cybersecurity in this country. And it is my hope that we can come together as a government and industry, Democrat and Republican—and work together to tackle this growing threat that we face.

With that, let me turn to Dr. Coburn for any remarks that he might want to add. Dr. Coburn.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Thank you, Mr. Chairman, and thank you for this hearing. I cannot let you get away with mentioning Delaware without mentioning the University of Tulsa, one of the leaders in cybersecurity in the country, and they are doing phenomenal work.

I also want to praise the administration for the Executive Order. I have done it before, but it shows what happens when government actually goes out to listen to industry and then works with industry to try to solve problems. And the whole framework for the Executive Order came out of this meeting of minds of what is the problem, what are the potential solutions, how do we get about that. And so this hearing today is an important hearing for us in terms of critical infrastructure and cybersecurity.

But we also have tremendous weaknesses. Dr. Schneck, this is the first time I have gotten to meet you. Everything I hear is great. I hope to come back out there and actually work with you directly at your facility. But, we run United States Computer Emergency Readiness Team (US–CERT) from Homeland Security, and they put out a notice on Windows XP. It is not going to be maintained anymore. But guess what agency has the largest number of Windows XP programs? Homeland Security.

And that is not to be critical. That is to say the problems are so big, and Homeland Security was brought together, and we are just now getting to the able-bodied capability that we need there to start addressing some of these internal problems.

The other thing that Senator Carper, and I have and we are working on the other side as well, is we are going to get you the capability to hire the people you need, and that is going to be on our next markup, I have been assured, and we are going to help that flow through Congress and gets to the President's desk, because one of the things you have to do is be able to compete with private industry for all these oversubscribed classes.

So I look forward to our hearings. I look forward to our second panel as well. I would also note we have a vote at 11 o'clock that is going to tie us up for 45 minutes to an hour, because there is a multitude of votes. So maybe we should get with it, and I will submit a written statement[1] for the record.

Chairman CARPER. Sounds great.

Very briefly, our witnesses: Dr. Schneck, is Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security. In this role, she is the chief cybersecurity official for DHS. Prior to joining DHS, Dr. Schneck worked at McAfee, Incorporated, where she was the chief technology officer for the global public sector.

Our second witness is Donna Dodson. Ms. Dodson is Chief Cybersecurity Officer for the National Institute of Standards and Technology at the Department of Commerce. Ms. Dodson also serves as the Division Chief of the Computer Security Division and Acting Executive Director of the National Cybersecurity Center of Excellence. In her position, Ms. Dodson oversees research programs to develop cybersecurity standards for Federal agencies and promotes the broader adoption of cybersecurity standards through public-private collaborations. Good to see you.

Our final witness is Stephen Caldwell. Mr. Caldwell is Director of Homeland Security and Justice Issues team at the Government Accountability Office (GAO). In his capacity he has worked on recent reports regarding the protection of critical infrastructure and the promotion of resiliency. Mr. Caldwell has over 30 years of experience at GAO, and we thank him and all of our witnesses for joining us today.

I want to thank Senator Johnson for joining us today. Very nice to see you.

Senator COBURN. I would just like unanimous consent to put into the record a report on the Federal Government's track record on

[1] The prepared statement of Senator Coburn appears in the Appendix on page 46.

cybersecurity and critical infrastructure[1] that was from February 4, 2014.

Chairman CARPER. Without objection.

All right. Dr. Schneck, you are the lead-off hitter. Swing away.

TESTIMONY OF PHYLLIS SCHNECK,[2] PH.D., DEPUTY UNDER SECRETARY FOR CYBERSECURITY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. SCHNECK. Thank you, and thank you for your very kind words. Good morning, again, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. It is an honor and a pleasure to be here before you today to talk about the Department of Homeland Security's——

Chairman CARPER. Is this the first time you have testified before a committee?

Ms. SCHNECK. It is my first time as a government witness, sir.

Chairman CARPER. OK. Fair enough.

Ms. SCHNECK. Which I have heard is a bit different. But it is a pleasure to be here to talk about the Department's work in cybersecurity and critical infrastructure.

We face a cyber adversary that is fast. They have no lawyers, no laws, nothing to protect, and they share information very easily. They execute when they want with an alacrity that we envy, and it is greater than ours. So in that spirit today, I will speak to you about our vision for the Department of Homeland Security, our work with the Executive Order, and with the fine people at NIST, and our implementation of the voluntary program, which we call the Critical Infrastructure Cybersecurity Community—C3 Voluntary Program.

I came to DHS 6 months ago. I came for the mission. I came to bridge the public and private. I come from a technical background in the private sector, and I was the authorizing person to share information with the government. That was hard. It was based in trust, and we knew we had to do it. And now that I have been in government, I have a whole new perspective of the challenges in government, and a top priority for me at the Department will be enhancing the trust that we have with our private sector stakeholders, as well as our Federal Government, our State and local stakeholders as well. Building that public confidence, leveraging the internal sibling organizations that we have with the U.S. Secret Service cybersecurity, the Coast Guard, the TSA, the Federal Emergency Management Agency (FEMA), our research and development, and, of course, our homeland security investigations, our internal law enforcement as well as our external partners with the Federal Bureau of Investigations (FBI) and the intelligence community, it is vital.

What we need to really improve our infrastructure resilience is speed. It is how do we increase that alacrity, and in that process I envision our National Cybersecurity and Communications Integration Center (NCCIC), as the core of that. How we have the gov-

[1] The report submitted by Senator Coburn appears in the Appendix on page 119.
[2] The prepared statement of Ms. Schneck appears in the Appendix on page 49.

ernment indicators that we get from our programs, such as EINSTEIN, Continuous Diagnostics and Mitigation, how we pull those together that only we can see because it is government, how we leverage our strengths and privacy and civil liberties, our ability to show the world everything that we do, full transparency, and work with the private sector through that trust that we need to build better partnerships, to create that common operating picture that the President requested.

We are already partway there in creating indicators, what I call a weather map. This is what the adversary cannot do, that situational awareness to turn our networks into more self-healing. Your body does not have a meeting to fight a cold. In the same way, our networks should not pass bad traffic. Right now we are passing malicious traffic at 320 gigs per second on world-class carrier grade routers to good people, and we need to work together in partnership. And one way we do that is with this framework.

I was on the first 6 months of this process with the great people at NIST as the private sector where all of our companies put our finest scientists to work with the government to create this broad set of guidelines for cybersecurity so that large companies could take what they know and put good practices into their suppliers, into their customers, and help raise the level of all cybersecurity to make our country safer.

One of the first things I did when I got to the Department is work with a team to take money to pay for Managed Security Services for State and local governments when they adopt the framework, logic being that in a year or so, when they are protected, because they sit on critical infrastructure information, private citizen information, and they know how much they have to protect but they are woefully underbudgeted. We will be protecting them while they use the concepts in the framework and the voluntary program and all the resources of DHS that come with adopting the framework—cyber resilience reviews, technical assistance—they will now be able to take that cybersecurity discussion to a level of risk-consequence, and likely have better budgeting decisions. Same with small to medium businesses to whom we have released a request for information saying how can you go forth and innovate, do what our country does best, take leadership and make elite security, new security products, services, things that protect us, but things that are affordable to those small to medium businesses, so that we all raise our level of security together.

We look forward to having that tie back to our vision because in that partnership, as we look at security holistically, as part of keeping the lights on and maintaining our way of life, part of infrastructure resilience, we build that trust and partnership across all sectors, that NCCIC continues to get information, that we cannot only provide in a weather map picture, which we already do, but also put out in real time so that when traffic is passed, networks know whether or not they should accept it. That is where we outdo the current alacrity of our adversary.

We have enjoyed the support of you and your Committee. We thank you for the confirmation of our Under Secretary Suzanne Spaulding. What we need is some statutory clarification of our role. To react more proactively and with greater alacrity, we need to

spend less time proving through a patchwork of legislation to our partners what our role actually is and more time just getting to it more quickly. That would help a lot, and also thank you for your kind words in the beginning about our workforce. I have had the opportunity and the honor to visit with Secretary Johnson some universities and some students. There is fine talent out there, and I know with our mission we could actually use our mission and outdo some of those salaries they are offered. But we have to have the flexibility and some additional competitiveness to bring them inside and see what we do and get them on board. That is our future.

So I thank you for the opportunity to briefly share our vision, to talk about the Executive Order, and I look forward to working more with you to make our country safer and more resilient. Thank you.

Chairman CARPER. That was an impressive debut.

Ms. SCHNECK. Thank you.

Chairman CARPER. Thank you.

Ms. Dodson, very nice to see you. Welcome. Please proceed.

TESTIMONY OF DONNA F. DODSON,[1] CHIEF CYBERSECURITY ADVISOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Ms. DODSON. Thank you. Chairman Carper, Ranking Member Coburn, and Senator Johnson, thank you for this opportunity to testify today on the National Institute of Standards and Technology's work through public-private partnerships in the area of cybersecurity.

As a scientific organization focused on promoting U.S. innovation and industrial competitiveness, we at NIST see ourselves as industry's laboratory with strong partnerships with the private sector driving all that we do.

As this Committee is well aware, NIST has spent the last year convening critical infrastructure sectors and relevant stakeholders to develop the Cybersecurity Framework. On February 12, Version 1.0 was released, along with a road map for future work in support of this effort.

From the start, NIST saw the framework as a tool that any organization in any one of the very critical infrastructure sectors could use to build strong cybersecurity programs. The intent was to assess the current capability of the market while offering a common language to address and manage cybersecurity risks. The voluntary nature of the program and the extensive private sector engagement has encouraged the widest set of stakeholders to come to the table and work collaboratively. This approach, with its reliance on consensus standards, has a proven track record. When industries and other private sector stakeholders get together and determine for themselves what standards are needed to ensure confidence and quality, those standards are much more likely to be adopted and implemented.

NIST began the framework development process with a request for information and received hundreds of submissions. Those sub-

[1] The prepared statement of Ms. Dodson appears in the Appendix on page 55.

missions provided a foundation for the framework. We followed this request with five workshops around the country with thousands of participants. Our approach was to gather feedback from participants, conduct analysis, and present those findings back to the community for additional refinement. Even the fundamental structure of the framework came from this engagement as an initial outline, was presented to the stakeholders, and then that outline was filled in at our workshops.

The result of this effort is a document that lays out critical elements of any cybersecurity program and then links those elements to proven best practices and protections for organizations to consider using while factoring in privacy and civil liberty needs.

The framework consists of three parts: the Framework Core, the body of existing practices that can help an organization answer fundamental questions, including how we are doing; the Framework Tiers that help to provide context on how an organization views cybersecurity risks; and the Framework Profiles that can be used to identify opportunities for improving cybersecurity posture by comparing a current state with a desired or target state. My written testimony has additional details on each of these pieces.

The framework structure will enable organizations to tailor plans to their specific needs and communicate them throughout their organization. Some companies may discover that an entire cybersecurity effort consists only of passwords and antivirus software with no real-time detection capability, and other companies may find the framework a useful tool for holding their key suppliers accountable for their practices.

As organizations use the framework, their experiences can then be reflected back to keep pace with changes in technology, threats, and other factors, and to incorporate lessons learned from its use and to ensure it is meeting national priorities.

Moving forward, NIST will continue to work with industry, DHS, and other government agencies to help organizations understand, use, and improve the framework.

Only 6 weeks in, we are aware of many organizations that are already using the framework and providing feedback to DHS and NIST. Phyllis has already discussed the great strides that DHS is making in working with sectors on more detailed operational guidance, which we will work with them to support.

We recognize that the cybersecurity challenge facing this Nation is greater than it has ever been. We are committed to working as part of the private-public sector team to address this challenge. In particular, NIST will continue to support a comprehensive set of technical solutions, standards, guidelines, and best practices that are necessary to address this challenge. Some of NIST's work will be conducted through other programs, including our work under the Federal Information Security and Management Act, the National Strategy for Trusted Identities in Cyberspace, and the National Cybersecurity Center of Excellence, as well as our research and development work.

Thank you for this opportunity to testify today, and I would be happy to answer any questions you may have.

Chairman CARPER. Ms. Dodson, thanks so much for your testimony and for being with us. Mr. Caldwell.

TESTIMONY OF STEPHEN L. CALDWELL,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Chairman Carper, Dr. Coburn, and Senator Johnson, thank you very much for asking GAO to come here today.

Chairman CARPER. How about Senator McCain over here?

Mr. CALDWELL. Oh, sorry, Senator McCain. I did not see you slip into the——

Chairman CARPER. He slipped in a little late, but he is here.

Senator COBURN. He is hard to miss.

Senator MCCAIN. I am insulted. [Laughter.]

Mr. CALDWELL. I am Steve Caldwell, and I am from GAO's Homeland Security Team, and I am in charge of our work on the physical protection of infrastructure. I am accompanied by Greg Wilshusen here, whom I think you know. He has testified before this Committee previously. He is in charge of GAO's work on cybersecurity. The reason both of us are here is we are bringing together some of our work on both the physical and the cybersecurity areas that deal with the partnership that we are talking about our report is here in the broader sense of trying to pull up some more generic lessons learned perhaps as we move forward with the new C3 initiative.

Since 2003, GAO has listed cybersecurity of critical infrastructure as a high-risk issue. There are several reasons for that. One of these is the importance of cybersecurity, as our dependence on it continues to grow and evolve. Also, cyber incidents continue to rise at a very quick pace, at least the ones we know about. Then the Federal Government continues to have a number of challenges in trying to deal with these incidents.

As noted, in the wake of the Presidential directives and the Executive Order last year, there is a new program, the C3 Voluntary Program here.

So today I am going to discuss key factors related to the partnership between the private sector and government that may provide lessons, moving forward. My statement is based on a broad body of GAO work that has included all 16 sectors of critical infrastructure. It has looked at protection against all hazards, both cyber and physical. It has looked at infrastructure largely owned by the private sector and programs that have used both a voluntary and a regulatory approach.

As a whole, the DHS partnership has made a lot of progress in terms of sharing threat, protection, and resiliency information with a wide variety of partners. These include other Federal agencies, State and local governments, and most importantly, with industry.

However, there have been many challenges, and we have noted these in our written statement. My written statement goes into both progress made in both the physical and cyber partnerships as well as several examples.

For example, our recommendations have asked DHS to seek better understanding and focus on what the expectations are of indus-

[1] The prepared statement of Mr. Caldwell appears in the Appendix on page 63.

try. We have asked DHS to identify and, where possible, clear some of the barriers to information sharing that we have found. We have asked DHS to determine why industry does not participate in some of the programs DHS runs so it has to go beyond those that participate to those that do not participate to find out why. We have also asked them to share information more broadly at the sector level and at the regional level. It should share information, not just with individual companies but in the broader sense of the grouping of companies. And we have also asked DHS to evaluate whether and how industry is actually using some of the assessments that DHS has provided, particularly in the voluntary programs. And then, finally, we are asking DHS to systematically assess the performance of the outreach efforts that they have to industry.

In closing, DHS has taken a number of steps to develop these partnerships, and these are critical for protection against both physical and cyber attacks. However, a lot more work remains, and we have kept the cybersecurity of infrastructure on our high-risk list in our last iteration of the list and anticipate that it will remain so as we move forward.

So until the Nation's most critical infrastructure systems have a better partnership with DHS these systems remain at risk.

That concludes my remarks. Mr. Wilshusen and I will be happy to answer any questions you may have. Thank you.

Chairman CARPER. Thank you very much.

Dr. Schneck, we just heard from Mr. Caldwell a series of, I will call them, "asks" from GAO. He says we have asked DHS to do this, and I think about a half dozen or so. Are you aware of those asks? And would you care to respond to what DHS is doing in light of them?

Ms. SCHNECK. Absolutely. And, first of all, thank you. We do a lot of work—again, my first 6 months with government, I am learning a lot, and I really appreciate the work of the GAO.

Chairman CARPER. They are good people.

Ms. SCHNECK. Absolutely, and I had the opportunity to work with them before. So there are many asks, some of which I have known a little of and some not, but we are in the first phase of, as Donna mentioned, an evolving program with the framework. So this is Phase 1. We are now into Phase 2. This is a living document. It will adapt and we will adapt to how industry and government need to raise the level of our security, evolve with our guidelines, and these metrics will evolve.

I think we are assessing right now our outreach. We are 2½ months in. We already have actually a checklist for our State and local as to who has adopted what parts of the framework, who is actually using services, who was before. We will be looking at doing something similar for the private sector, and certainly on the government side, absolutely. So we are very much on top of that, but also tracking in partnership, because the success of this, as I saw in the first phase as the private sector, comes from the fact that the private sector is very bought in. They know that they designed this thing with us, with NIST, and they have a lot of trust in that. So we want to maintain their input as we build how we rate the success.

Chairman CARPER. Could you just describe for us in your own words the role—we have the framework, we have the blueprint, the road map. It has been well received in a lot of circles. What are some of the criticisms you have heard of it? This is for anybody. What are the criticisms we have heard of the process and the product to date? I have not heard any, and there must be some.

Ms. DODSON. So as we were beginning the development of the framework, I think people were concerned if this would truly be a private-public partnership, or did the government have the answer in its back pocket that it was going to put out and put forward. Through the process that we put together with industry and the iterative and the constant communication from one workshop to the next workshop, they could see the development of the framework and the inputs that we received and how we got to the end stage.

People are always concerned about cost, and so as you look at the framework development, we took a risk management approach so that it is integrated in with your entire business. And really that work with the private industry on the appropriate set of standards and best practices to put in there, there is an element of cost there, and they can balance that with the risks that they see and the need to protect their information.

So those are two of the major concerns that we heard during the development process of the framework and how we addressed those collectively across the government.

Chairman CARPER. All right. Thank you.

Dr. Schneck, talk to us a little bit about the role of DHS going forward in terms of implementing the framework and figuring out who needs some help in implementing maybe small and mid-sized businesses, maybe even some larger ones. How do you identify them? Do they just step forward and say, "Well, we need some help. What can you do for us? and then you have a conversation?" How does that work?

Also, in terms of what you need at DHS to do that job, the kind of resources that you need, be they people, the kind of people skills that Dr. Coburn talked about, technology, authorization, maybe things you need from us, talk about those, what your needs are to be able to meet your responsibilities in implementing the framework.

Ms. SCHNECK. OK. I will start with DHS' role, the response and mitigation to cyber attacks focused on critical infrastructure resilience, basically to protect that holistic all-hazards approach, and really looking at cyber discussion as that risk-consequence equation. Going back to what Dr. Gallagher said about equating cybersecurity and business practice, when are we going to get there? And I think our role is twofold.

One is on the people side really engaging those partnerships. To Donna's point, there was a lot of skepticism. Will this really be a partnership? And part of our role in working with NIST and others is to make sure that the private sector is at the table in helping those discussions and taking their lead on what it is going to take to, No. 1, help the providers make better technology, to help us innovate and drive those markets economically; and the other is how do—to your other point on small to medium business, that is a

huge risk. I testified on that in another capacity some years ago. These are companies that have no idea in many cases that they have something to protect, and yet they are connecting to everybody else, making the rest of us not secure, with very small budgets.

I went to Silicon Valley 2 weeks ago to talk to our venture capital community, to talk to our innovators out there about how they can protect those assets they are funding and growing.

So our role in DHS on the people side is really to engage, to partner, to build that trust, and to use those qualities that we leverage most—the privacy, the civil liberties, the transparency—so that when we bring people and information together, we can push it out as fast as possible to help stop bad things getting to good people. But we can also be a resource for people to learn.

On your next question about implementing the framework, we have a very aggressive schedule on helping. We are reaching out to small to medium business through the Chamber, through other organizations, obviously reaching out to the larger businesses through our Conservative Political Action Committee (CPAC) partnerships with all 18 critical infrastructures, certainly on our Federal civilian side working with all of the agencies and with the State and local through the Multi-State Information Sharing and Analysis Center (MS–ISAC), so certainly reaching everybody. Everybody has different sensitivities. Everybody has different things they need to see. And working through all of that through different teams that are joined together.

And quickly to cover on the workforce, there is great talent out there. We need everything from technical——

Chairman CARPER. When you say "out there," out where?

Ms. SCHNECK. The universities that——

Chairman CARPER. Within DHS or outside?

Ms. SCHNECK. Both.

Chairman CARPER. OK.

Ms. SCHNECK. And I will say for all the skeptics, I walked into one of the finest teams on the planet.

Chairman CARPER. Really?

Ms. SCHNECK. So those who think that government is not smart, they are wrong. What we need is more people like the ones we have, some more technical resources like we have in our US–CERT, because more and more we have those teams that fly off and help people respond to attacks. We need to have more of that. And there is a spectrum of skill sets. We need the cybersecurity experts. We also need folks that are skilled in analytics. We need policy people. And that combination of talent and people that work with us, with our Science and Technology Directorate, through Research and Development (R&D), need to look at a holistic view of what we can do with our partnerships, what we can do across cybersecurity across DHS, and have a mind-set of where we can go next. This is how we get faster from our adversary, and I have had the opportunity, as I mentioned, with Secretary Johnson to meet some people that I believe fit that bill. And I believe our mission can meet what their other salary offers can meet in a different way.

Chairman CARPER. How can we help? Dr. Coburn mentioned briefly one idea, and that is to make sure you are able to attract and retain the kind of talent that you need in this arena. But whether it is in that regard or some other regard, how can we help you meet the responsibilities that you are facing?

Ms. SCHNECK. The onboarding process, if we could make that easier, give us a little bit more money to hire, a little bit stronger hiring authorities to make things more competitive for us, because our mission meets the salary. People say that good talent does not come because we cannot pay them. Sometimes we can make up some of that gap with our mission, but the rest of the gap and the long process and what it takes to come work for government, if you could help us make that easier, give us some additional authorities to bring great people on, that will help our overall partnership. And I believe that goes to the safety of our Nation.

Chairman CARPER. Good. Thanks so much. Dr. Coburn.

Senator COBURN. One of the words that you spoke a minute ago was maintain input from the private sector. And what I hear from the private sector is this inherent worry that we get to the implementation phase and this is no longer a voluntary program but a mandatory program. Talk to us about that.

Ms. SCHNECK. Thank you for that question because it is something that we work with every day, because we heard it every day from our stakeholders. The main goal of this framework was to engage the private sector to drive this with their innovation, with their picture, and to get us as a country together, public and private. There is no better incentive than actual security and safety.

At the White House anniversary of the framework on February 12 of this year as well as the day of the beginning of the launch of the voluntary program to adopt the framework, we had several CEOs in attendance of some of the major large companies, and one actually said his major incentive was fear and that he would be helping us to implement this.

So other ways that we are looking at this is how do we continually in a phased approach maintain the private sector's involvement as we do the adoption. We will learn. We are putting all of our resources out to the private sector. We are not asking them to report to us if they have used it or not. We want to look at our outreach. We want to study our metrics, stay involved with the large companies that are—and this is very key to me—asking their suppliers to be more secure so that when you connect to a smaller company, you do not endanger the larger company, and requiring of their customers, same with the State and local. And a lot of basic cyber hygiene and guidelines that are mentioned in this framework could have prevented a lot of the attacks that we have seen thus far.

Senator COBURN. Thank you. Talking a little bit about government, hygiene in the government, it is a big problem, isn't it? How do we solve that?

Ms. SCHNECK. Wow. So one approach that I would look at—and you mentioned the Windows XP, so that is a great example. This is a critical issue that is affecting everybody. DHS has worked with Federal agencies to get this awareness out. We have a great partnership between the National Protection and Programs Directorate,

where I sit, and our Chief Information Officer (CIO). Our great new Chief Information Security Officer (CISO) Jeff Eisensmith, and CIO Luke McCormack and I talk all the time, because, candidly, there is no sweeter network than DHS.gov to learn from who is trying to attack us. And then we put that knowledge into how we protect everybody else.

On the XP issue, the migration to Windows 7 for us is expected to be complete before the end of the security updates for XP, and I know that DHS long before I got here put that warning out to all other agencies. So that is one way I think DHS protects our other agencies.

The other is in programs such as EINSTEIN, with simple network protection intrusion, prevention and detection. But the ability to understand with our information—again, we see all the networks we protect, so all that information that large view in the Concept of Operations (CONOPS) for cyber from that NCCIC goes into the protection of every single agency that we protect. And then every time we see something, we learn something from it, and that goes to protect everyone else, and we can push that information out as well to State and local. So that hygiene in government can come back to our programs.

I also want to call out on that same note Continuous Diagnostics and Mitigation. That is near and dear to me because it takes the 3-year book of compliance that I called a "doorstop" when I was in the private sector; it takes people's resources to build this one book of compliance that says at this moment in time this is how my network looked. Continuous Diagnostics and Mitigation changes your network into an immune system. At any given moment, it will understand, detect, and attack something that is bad and report on it. So you can save your strongest minds to hunt for the most malicious actors.

So in government, we are taking large strides toward that hygiene. All of that fits within the guidelines of the framework. And then certainly taking that data from Government that we learn and pushing it out to private sector. So we think Government hygiene will uplift everybody else, and we certainly hold ourselves to higher standards than others at DHS.

Senator COBURN. There has been some maybe not criticism but some questions about the efficacy of EINSTEIN. Do you feel comfortable that it is where it needs to be?

Ms. SCHNECK. I do. So 6 months ago, when I came in, one of the first things I did was learn the history and then the current path of where we are. There were, of course, some hiccups, as in any large technology program that I have seen all my life. But now we have our second service provider on. In fact, now that that service provider is signed up to provide Einstein 3 Accelerated (E3A) accelerated services, which is used in prevention, we at DHS will be leveraging those services as well.

We are finally at a point as well where we are getting enough data and protecting enough agencies—I think about a quarter now of the seats in the government—and a lot of that depends on, again, getting other service providers signed up, but I think we are at a point where we are now looking at the more interesting topic,

if you will, which is how do we use the data that we are collecting from government to give it to the private sector.

Senator COBURN. Sure.

Ms. SCHNECK. For example, programs such as Enhanced Cybersecurity Services, which allow us to protect the private sector with classified information, as well as take unclassified information but that we learn from the EINSTEIN program in government and push that out in real time with regular trafficks, so that as traffic flows through the network, other parts of the network and other devices know not to accept it if it is going to hurt you.

So to wrap up, government hygiene I think is important, and it affects everybody.

Senator COBURN. So it is important not just to maintain the input from the private sector, but also to maintain the trust of the private sector that what you have provided to them is worth them having.

Ms. SCHNECK. Oh, absolutely, because, again, someone like me, 6 months ago in a company, was given the ability and the authorization to use my own judgment when we should talk with government, and I was always asked what are we getting back, what are they doing. So that is in both human time, what are we going to learn from different government agencies by sharing; and then in real time, the government and I believe DHS uniquely, because of our emphasis on privacy, civil liberties, and transparency, and our NCCIC, has the ability to correlate that data and learn a lot from private sector, combine that with what we as only government can see, and push that out faster than our adversaries could hurt us.

Senator COBURN. And so in your thought pattern right now, as long as you can keep the voluntary compliance and working relationship on a basis of trust and value, we are not looking at hard regs mandated by the Federal Government for this is how you will do this.

Ms. SCHNECK. We are focused on voluntary engagement, learning as much as we can from the private sector, and pushing as much correlated data out as we can.

Senator COBURN. All right. Thank you.

Ms. SCHNECK. Thank you.

Chairman CARPER. Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman. Ms. Schneck, welcome.

Let me pick up where Dr. Coburn left off there. I have been here 3 years now, and we have been talking about cybersecurity. I was actually in the meeting with a bunch of Senators trying to hammer out a cybersecurity bill. A pretty prevalent attitude in that room was that businesses, the private sector, needs to be forced into protecting their cyber assets. Is that your experience in the private sector?

Ms. SCHNECK. So I came from a large cyber provider, so, no, we did not need to be forced to protect cyber assets. But I can tell you that our customers did not either. They had either experienced a breach or knew enough to know that they would experience a breach, and many in the field say that there are two kinds of companies and entities right now: those who know they are compromised and those who do not.

So the issue is how we raise cybersecurity to a business discussion. I think that the framework and the voluntary program will get it to the board room, because it becomes part of the risk. We do not force people to lock their doors, and yet they do. So this is part of a culture of security that has been talked about for 12 years. I think Howard Schmidt is the first person to use that phrase back in 2000, 2001, or 2002. And looking at how we continue to engage that private sector innovation, drive the market.

Once NIST engaged with the private sector, they sent out their best and their brightest for 3 to 4 days at a time to workshops that required long flights, and they are continuing to remain involved because they see the importance, not just for their brand reputation but for their customers and, candidly, as part of our Nation's network and our global assets.

Senator JOHNSON. Well, it was certainly my attitude, and trust me, I was the minority view, that I really think businesses want to protect their cyber assets and actually look to government, acknowledging the fact that the government has an awful lot to offer. And so I have really been pleased with what NIST is trying to do, make this a voluntary approach. It is the way to go. If we can facilitate cybersecurity versus dictate it, I think this will work. If we try and dictate it, I think the private sector shuts down.

Over these 3 years, it seems like the No. 1 component or the first priority is really to facilitate information sharing. Ms. Schneck, you talked about the need for speed. What is the greatest inhibitor to get that free flow, that rapid, the speedy information sharing that is required if we are going to detect cyber threats and try and contain them as much as possible.

Ms. SCHNECK. I have an optimistic view of that, and there are pockets in the private sector that can already do this. That is how I know we can build it, and that is how I know how—I built one of those in my previous life—where the analysis of data can be in real time pushed out with traffic.

I think our job as government, and especially with DHS as a lead civilian agency for this, with the ability, again, to do it right, with privacy experts and civil liberties, and show the world exactly how we do it, we have the ability to correlate information and get a global view of what traffic might be OK and what might not be, and to literally pass that at machine speed. Just as you send an e-mail——

Senator JOHNSON. But, again, businesses have to feel comfortable to share that information. Isn't liability protection a big problem in terms of businesses not being willing to share that? And isn't that something Congress needs to do?

Ms. SCHNECK. So we look at liability protection. I can give you an anecdote from my previous life. This is something that would have helped us, because I was often in situations where, as company or country, and can you share, the lawyer will not let you, but you know that the information you have from the research you do could help a lot of people. So I know the administration is looking at targeted liability protection, and, again, my perspectives have changed a bit since I have come over to government, because I see some of the different challenges. And part of what I want to do is bridge that, and that is why I want to build that trust.

And I think that the targeted liability protection that the administration is looking at right now would help us because it would protect companies in the instances defined to share information, and they would not get hurt by that and would not be held liable, nor would their shareholders, if—for example, in my case, when I did this, a sector could be exposed for having potential liabilities. But it would not be so broad that it threatens even the optics or the perception of threatening our privacy and civil liberties because we are fighting to protect, again, our way of life. So it is a balance.

Senator JOHNSON. The devil will be in the details on that one.

First of all, I am pleased to hear that you appreciate the talent that is already in your agency. That is good to hear. I am intrigued, by the way. I really appreciate the fact that you are willing to leave probably a pretty good-paying job and come in here and do work for the Federal Government, pretty important work.

Ms. SCHNECK. Thank you.

Senator JOHNSON. Let me just ask you, if you had to go through the confirmation process, would you have decided to make that switch?

Ms. SCHNECK. If I had to go through the confirmation process? So when——

Senator JOHNSON. Did you go through the confirmation process? My information is you did not.

Ms. SCHNECK. Not the Senate confirmation, no, sir.

Senator JOHNSON. Correct. But if you——

Ms. SCHNECK. But I would have done it anyway.

Senator JOHNSON. But had you gone through the confirmation process, would that have prevented you from considering a position here in the administration?

Ms. SCHNECK. No.

Senator JOHNSON. OK. In terms of attracting other people into government, into these high-tech positions, certainly there is kind of the mission challenge that is attractive, but, again, there are a lot of good-paying jobs out in the private sector. Can you speak to what kind of dollar differences we are talking about?

Ms. SCHNECK. Oh, wow. So, again, all of that, it depends on——

Senator JOHNSON. I am a business guy, so I focus in on some of those practical concerns.

Ms. SCHNECK. So in many cases, sir, there are six-figure differences, and that is before the stock. However, I think there is a much more important—it is not always that way, but there is a much bigger, I think, calling, if you will, and that is that when you get to government and you can—and I only learned this 6 months ago, but how much people in government do so that someone in my position never knew it got done and just felt safe every day. I think that having that other piece of knowledge helps bridge the gaps that we need to bridge to keep our economy—to let our private sector drive innovation to keep our country in leadership in science, and all of that will make us more secure. And so what I would love to do is be able to pull some more people from the private sector and say, "Come see what I learned, and come join our team and help us." I know that our mission can pull them.

From what I am told, the hiring process is very difficult, and, if, again, we could get that help from Dr. Coburn and from the Committee——

Senator JOHNSON. OK. That is really the point I am trying to make.

Having come from the private sector, which obviously has bureaucratic problems as well, can you just compare and contrast a little bit in terms of what you see, what your viewpoint is, comparing bureaucracy in the private sector versus bureaucracy here in government? Because, again, this has been an urgent need since I have been here, and even before that. This is 3 years. We are still moving forward. We are still talking pretty much about the same issues, although there has been some real advancements because of the Executive Order and NIST, and I appreciate that. But we are still, it seems like we certainly have a ways to go.

Ms. SCHNECK. So do you mean in the hiring or in the technology?

Senator JOHNSON. I am talking about just in terms of moving a process forward and the bureaucracy versus the private sector versus government.

Ms. SCHNECK. So in my short 6 months here, I have learned that working with our partners across the Department as well as across agencies and certainly with committees such as this is the best way to get things done because you build support for what needs to get done, you target your budget, your blueprints and your outlook, your strategic plan toward what you feel needs to get done. In a company, I think that sometimes things move a little bit faster. But bringing that together—and that is what companies can do best. That is why they can innovate so quickly. But then, again, there are rules and reasons why we have government processes. I have had the opportunity and honor to start to understand some of that. It keeps government honest. And we do have a lot of information and deal with very large budgets. I think that is fair.

But, again, bridging that, building that partnership, building that balance, I have seen both bureaucracies, and I know we can work together, and I plan to get that done with your help. We need your help.

Senator JOHNSON. OK. Thank you.

Thanks, Mr. Chairman.

Chairman CARPER. Thank you, Senator Johnson. Senator McCain.

Senator MCCAIN. Well, thank you, and I thank the witnesses.

Ms. Schneck, you said that would not have deterred you, having to go through the confirmation process, but I guarantee you are just as happy you did not. [Laughter.]

Let me ask all three witnesses, isn't it true that current trends indicate that the incidence of cyber attacks and incidence of breaches of cybersecurity will continue to increase in terms of frequency and gravity for the next 3 years and the costs will increase more quickly than the benefits? Would you agree with that assessment?

Ms. SCHNECK. So I have not seen those numbers or the source. I do think cyber attacks are increasing. I do think the gravity is increasing. And we see everything on the spectrum from making noise to preventing business to actual destruction.

Senator MCCAIN. Ms. Dodson.

Ms. DODSON. So when we started the development of the framework——

Senator MCCAIN. My question is: Do you believe that they are increasing?

Ms. DODSON. So yes, we do believe that they are increasing, and that is why the framework addresses resiliency, not just stopping the attacks but that protect, detect, respond, and recover capability that are outlined in the framework, because that resiliency is very important.

Senator MCCAIN. Thank you. Mr. Caldwell.

Mr. CALDWELL. Senator McCain, hopefully I can make up for my omission at the beginning——

Senator MCCAIN. Inexcusable. [Laughter.]

Mr. CALDWELL. The data that we use, which is from CERT, certainly shows a striking increase in incident numbers.

Senator MCCAIN. And more than 100 countries are cyber capable. And if you put it into different categories—and there are different ways of doing that, but let me try this: Political activism, organized crime, intellectual property theft, espionage, disruption of service, and destruction of property—which of those are our highest priorities, would you say, Dr. Schneck?

Ms. SCHNECK. I believe that resilience against all of them. They are all happening. If we prioritize toward one, the adversary will go after——

Senator MCCAIN. One or two is fine.

Ms. SCHNECK. So the ones that harm our way of life, the destruction for me, and certainly for the business.

Ms. DODSON. So I agree with Phyllis that look at resiliency is critical, and those things that really affect our way of life and those things that touch our life, and it is a big challenge as we look at the explosion of information technology across all aspects of our life.

Mr. CALDWELL. Senator McCain, really the priorities on those threats would vary a lot. Obviously, in government you have to worry about espionage of national secrets. If you are big company, you are worried about data breaches, dealing with your consumers and your clients. If your business is dependent on the innovation end, you are worried about the stealing of your intellectual property.

Senator MCCAIN. And I think we all conclude that the cybersecurity is an issue of transcendent importance.

Mr. Caldwell, the cybersecurity budget is about $1.5 billion. It is less than 5 percent of the total DHS budget. We do not like to talk just in terms of money, but money is a very significant factor. Do you think that that is sufficient priority of cybersecurity, that amount of money?

Mr. CALDWELL. I am going to ask Greg Wilshusen to address that. He does most of our cyber work within GAO.

Mr. WILSHUSEN. Good morning. I would say that, we did not address the budget per se, whether that particular amount is enough. One of the things that governmentwide has been reported is that government spending toward information security has been around $13 to $15 billion out of about $70 to $80 billion spent on informa-

tion technology (IT). So it has been about 18 percent, as has been reported by the Office of Management and Budget (OMB). Within the Department of Homeland Security, I do not know if I could actually say that that is the accurate amount or the total amount that should be spent.

Clearly, the Department has many responsibilities and needs to do a better job in certain areas in terms of providing better support to the Federal agencies as well as to critical infrastructure. If that is a matter of budget, I think we talked earlier about there are some needs for top talented people to continue to come to the Department.

Senator MCCAIN. Thank you. I, like Senator Carper and Senator Johnson, have spent many hours in meetings trying to formulate cybersecurity legislation. We bump up into various problem areas—privacy versus national security, what the role of private enterprise is. We continue to address this in a circular fashion.

One of the reasons is because we have oversight overlap of so many different committees that have responsibilities—the Judiciary Committee, Armed Services Committee, this Committee, and probably the Commerce Committee and many others.

Given the gravity of this challenge that we face, I have been arguing for a Select Committee. I count some 30 pieces of legislation that have already been introduced in both Houses, and, of course, none of them are going anywhere.

Mr. Caldwell, does GAO have a thought on that subject?

Mr. WILSHUSEN. Certainly there are a number of Congressional committees that have oversight of the Department. I believe the Department would probably be better positioned to determine what impact that has on it. But we do testify before a number of committees on this subject. But it is up to Congress to organize as it sees fit in terms of how it provides oversight.

Senator MCCAIN. Thank you.

Ms. Schneck, should we shift the focus to telecommunications companies and Internet Service Providers (ISPs) and examine whether they could be doing more to monitor the various cyber threats coming through their infrastructure?

Ms. SCHNECK. So cybersecurity is a shared responsibility. We all have a piece throughout government and the private sector. In my experience, the telecoms have done a lot. They have really stepped up and helped, for example, in botnets, which is when the adversary ties together tens of thousands of machines sometimes, compromises them, and tells them to send a lot of traffic all to one or two places. That is called "distributed denial of service," and it prevents business from being done because imagine too much water from a fire hose going into a straw. It just cannot be handled.

One of the things that the ISPs have stepped up to help us do with the NCCIC is when we use our trusted partnerships to coordinate and understand which machines are causing the harm, the ISPs actually are online ready there to take the information from us and help distribute that through their networks since they are carrying all of this traffic. So that is one way they have partnered. They are very engaged in many of the different public-private partnerships, and I hope that other sectors—some already are and

some are not—but, again, they are one piece, and, again, it is a shared responsibility.

Senator MCCAIN. Well, it is my conclusion, after looking at where different personnel assigned to cybersecurity responsibilities are spread throughout the Federal Government, we have Cybersecurity Command in the Department of Defense (DOD), we have you, we have other agencies of government all who have a cybersecurity responsibility. And, frankly, I do not see the coordination between those different agencies of government that I think would increase dramatically our effectiveness. And if we engage in legislation, which we have tried to do without success, I would argue that that has to be part of any legislation that we enact.

If you view this threat with the gravity that many of us do now, then it may require a reorganization such as we carried out after 9/11, which is the reason why this Committee and the Department of Homeland Security is in being. I hope that you will contemplate that kind of option as we examine all options, because one thing we do agree on, this problem is going to get a lot worse before it gets better.

I thank you, Mr. Chairman.

Chairman CARPER. We are going to start voting here very shortly, and my inclination—I checked with Dr. Coburn to see what he thought, and we think we will be here until about 11:15 for the first panel. Then we will excuse you. We will run to vote, and we will have a series of votes and come back as soon as we can, my hope is around noon. But we will see how that works out.

I would say to our second panel, those of you that are here, thank you for joining us. Please be patient with us.

I want to go back to something that I think you said maybe in response to Senator McCain, Dr. Schneck, and I think you mentioned the words "targeted liability protection." Senator McCain knows, as do my other colleagues, Dr. Coburn especially, that one of the issues that has made it difficult for us to put together any kind of comprehensive cybersecurity policy has been our inability to agree on what kind of liability is appropriate. And Secretary Johnson mentioned to me last week that he has been noodling on this and thinking it through as an attorney what might make sense, and obviously you have as well. Just think out loud for—and I am going to take about 3 minutes, and then turn it over to Dr. Coburn. But think out loud for us about what form that targeted liability protection might take, looking at your private sector experience, which you have alluded to, and your current role.

Ms. SCHNECK. So thank you. The end goal is to get the combined set of information. You have a wide set of companies that see a lot, some that make cyber products, some that use them, some across all different sectors from electric to water. We need to know what they see. We need to know what they know. And they need to know what we see from across, so how do we build that trust?

It is very difficult coming from inside of a company to make an attorney feel comfortable—and I am not a lawyer, so I can say that—with the idea that I am going to pick up the phone and call someone in government when, again, a lot of these companies are not based in Washington so there is—and that is why I have spent some time in California. There is a lack of understanding as to

what happens in Washington. And we have tried as a Department to put a friendly customer service face and engage other areas of the country because of this.

We have to get the general counsels to be comfortable with the fact that information is going to come—not intellectual property but information about awareness and cyber events, whether it is their breach or something else that they are seeing or building. We have to have the lawyers comfortable with that transfer of information.

I was held accountable. I trusted, candidly, Larry Zelvin in our NCCIC. I called him and I called some folks at the FBI that I knew, and those were trusted relationships. I could have lost my job if something went wrong.

DHS, FBI and the Secret Service has always handled my information the way we asked. We could control whether it went to government, whether it went to industry. But, again, we wanted to be protected from getting hurt. If you tell the government that the electric sector has—we have seen activity across the electric sector, as we saw in Night Dragon in 2011, where five oil and gas companies had their oil exfiltration diagrams shipped off to another country unknowingly. We wanted to issue a warning to the whole sector, and the lawyers had a very difficult time with that because they felt that the shareholders in that sector would suffer the next morning and it would be the company's fault.

So that is a case where some protection would be needed, not liability for everything on the planet, but liability protection for that case. And I believe that is part of what the administration means by targeted liability. And if those companies can feel comfortable in those situations, we believe more information will come in that we can then use to protect.

Right now it is game on for the adversary because everybody is afraid to share information. And if we wait and do not share this information and do not engage these partnerships and do not leverage the work of NIST and this framework, we let the adversary get far too ahead.

Chairman CARPER. All right. Well, this is a conversation we are going to want to continue.

Ms. SCHNECK. Yes.

Chairman CARPER. And if we can solve this one, I think we will move a long ways toward where were need to go in this arena.

Ms. SCHNECK. Thank you.

Chairman CARPER. Dr. Coburn.

Senator COBURN. One of the assumptions that has changed during my lifetime as a citizen of this country is the assumption in government that people are going to do something wrong rather than they are going to do something right. And it has been one of the most discouraging things I have ever seen in our country. It is because basically the vast majority of the people in this country want to do everything right. They do not want to do it wrong. But government's interface with them works under the assumption that they have done it wrong, now prove that you have done it right. And that is the key where we are on this liability.

Just for example, let us take two of the large Internet service providers. Unlimited liability, that is a great focused thing, but

look what we lose when we start limiting the ability of two ISPs who are working on something back and forth to actually really talk a lot back and forth, and the Justice Department comes in with their Antitrust Division and says, "Hey, wait a minute, you have to prove that that was necessary for cybersecurity rather than you guys colluding to keep somebody out."

And that is where this gets sticky. It is like Senator Johnson said. The fact is that I know right now ISP providers are talking back and forth without any immunity because it is the best thing to do for the country to protect us. And yet what we are finding is resistance here to give them that kind of broad legal liability because we do not trust them. We do not trust them to do what is best for the country as a whole, and we think they are always self-centered, they are only going to do what is good for them. And we have already seen in the cyber arena that is not true. And yet this whole concept of a very narrow limited liability is based on the assumption that we do not trust them, and so, therefore, we can only give you limited liability. And what we are going to do, if we do a very narrow limited liability, we are not going to get where you have espoused we want to get, because their same lawyer is going to say, no, you got to have this there, so, therefore, you can no longer do this.

So that is the downside to this, and it is important that that gets communicated up the chain when we start talking about specific limited liabilities versus general liabilities. And the proof is in the pudding of what are your actions directed toward and what are you trying to accomplish, not a specific event, because if it is only event related, we are going to lose. We are going to lose in this battle.

Mr. Caldwell, I want to talk to you a little bit—and I am saying this based on hindsight, and it is no reflection on DHS today. But there is a great example on how not to do something. It is called the Chemical Facility Anti-Terrorism Standards (CFATS), the chemical facility security act. And I just wondered, have you looked at that at all? We spent billions. We have not inspected the first chemical plant. We did not use this proactive Executive Order style that the President used in terms of creating a partnership. We did not listen to industry. What we did is create a bureaucracy and spent a bunch of money. And today we still have not accomplished what we need to in terms of chemical facilities.

So my question to you—I do not think that DHS has been effective at CFATS. It is better. I admit that. The guy that is running it today is far superior to what we had in the past. It is improving. Do you think CFATS would have been better if we had done a public-private partnership much like we have done in terms of cyber?

Mr. CALDWELL. I think it is hard to say. I will say a couple things about CFATS.

We have done a number of reports about it, and I would agree the last 2 years they have made a lot of progress, and a lot of it has been actually tracking what they are doing and paying attention to it and trying to work with industry. So there has been—they are getting closer to those compliance inspections for those facilities that are deemed to be high risk.

There have been a lot of distractions along the way. I think a lot of the problem was actually setting up the bureaucracy in the first

place in terms of deciding what they were going to do, what kind of people they needed, what kind of inspections they were going to do, and how they were going to do their risk analysis. We have made a number of recommendations that they have taken pretty seriously and they are moving toward.

It was very slow, and that is maybe a cautionary tale of going down a regulatory path, that there is a lot of structure to a government regulatory process, whether it is through the rulemaking process or other things that take a lot of time. And I think that is some of it. But I think a lot of it can be traced back to starting from scratch.

For example, the Coast Guard, they had the Maritime Transportation Security Act. They had that up running within about 18 months, but you have to remember they also had a lot of regulatory structure that related to the maritime sector. They had people that already——

Senator COBURN. Well, they also have a different management structure. You will do it, or you are getting booted out of the Coast Guard. That is different.

Mr. CALDWELL. Yes, sir.

Senator COBURN. Let me go back to my original point.

Mr. CALDWELL. Please.

Senator COBURN. Had we started out CFATS with the framework that said we are going to bring all the industry together and say how do we best solve this problem—that is not what we did with CFATS. And that is what we are trying to do now. I understand that. But it is my point, and it is a great lesson for us, and I think we have that dynamic going now in cybersecurity. But in this one, it is in the best interest of a chemical company to not have exposure. But the assumption under CFATS, which goes back to what I said before, is prove that you are not, rather than the assumption is we are going to assume you are and we are going to have to show you where you are not, and let us do this in a cooperative manner so that when we regulate you, we can take what we learn from XYZ Company and put it over to ABC Company, and we will come with judgment, because that is what was lacking with CFATS. There was no judgment because there was no knowledge, because we did not listen to industry, who at their own best interest want to protect their facilities.

Mr. CALDWELL. I think the——

Chairman CARPER. I am going to ask you to be very brief. I want to make sure that Senator Johnson has a chance to ask a question or two before we close. Go ahead, very briefly.

Mr. CALDWELL. So, briefly, I think industry was engaged with government when CFATS was created. I think one of the problems that happened is after the law went into place, then government kind of went into this quiet period where that engagement kind of stopped, and maybe that is where when we move forward with this, we have to make sure that engagement stays at a high level all the way through.

Senator COBURN. All right.

Chairman CARPER. Good point. Senator Johnson.

Senator JOHNSON. Thank you. I want to drill down on the liability protection issue. Right now it seems to me like we are erring

on the side of limited liability protection or no liability protection. As a result, we are not getting the information that everybody believes is absolutely crucial if we are going to provide cybersecurity. Correct?

Ms. SCHNECK. I would add that a lot of information is already being shared through our Cyber Information Sharing and Collaboration Program (CISCP) programs.

Senator JOHNSON. But not enough.

Ms. SCHNECK. There is more. And coming from the other side, I know why some of those lawyers want liability protection. We need a balance.

Senator JOHNSON. So let me complete my question. What would be wrong with erring on the side of too much liability protection so we would get the information, so we would, complete this urgent need to provide greater cybersecurity? What would be wrong in just erring on the side of maybe too much liability protection? What is the cost? What is the damage in doing that, other than to the trial lawyers?

Ms. SCHNECK. So that is hard for me as a nerd, not a lawyer, but I am open to have the conversation. Again, you know my goal. It is to bring all the information together. And I need to work with our experts in the administration and in Congress to understand what our folks at NIST and DHS have——

Senator JOHNSON. But, again, if we provide too much liability protection, that means companies will not be able to be sued as readily, correct? Isn't that the——

Ms. SCHNECK. We do not want companies getting sued. No, we do not. We want information shared. I need——

Senator JOHNSON. Why would we withhold a broader level of liability protection other than for that reason?

Ms. SCHNECK. I need to understand all the legal issues around that, and, again——

Senator JOHNSON. Let us just walk through when companies get sued, who pays for that. I just want to so people understand. If a company gets sued and they pay a big old fine to the Federal Government or a great big class action suit, who really bears the cost of that litigation?

Ms. SCHNECK. We absolutely all do, and the bad guys win. It is a terrible situation.

Senator JOHNSON. We all do.

Ms. SCHNECK. Yes.

Senator JOHNSON. So every consumer ends up paying higher prices, correct.

Ms. SCHNECK. Absolutely. It is a terrible situation. It is——

Senator JOHNSON. Now, who benefits from that liability? I mean, when somebody sues successfully, who benefits?

Ms. SCHNECK. I am not a lawyer, but probably the lawyers.

Senator JOHNSON. Certainly trial lawyers on a contingency fee, they make a lot of money, correct?

Ms. SCHNECK. Probably.

Senator JOHNSON. Every now and again, when it is a class action, the members in that class might get, oh, a couple pennies?

Ms. SCHNECK. I actually do not know.

Senator JOHNSON. Well, that is really, in effect, what happens. So, again, I just want us to be really realistic in terms of what is happening here. By not providing broader liability protection, we are putting our cyber assets at risk. And what we are doing is we are protecting the ability of trial lawyers to get big old fees. Generally the class action plaintiffs get very little. And when we do have these huge settlements, it is American consumers overall that pay the higher costs.

Ms. SCHNECK. And this is why the adversary is winning because they have no lawyers——

Senator JOHNSON. Precisely. So, again, I think it is just important that we understand what is happening when we refuse to provide broader liability protection so we can actually get the information that we need to provide cybersecurity.

Ms. SCHNECK. And that is why we need to have a conversation, before anybody refuses anything. But, again, we need the experts from the science side, the legal side, the administration to find that balance, because we do not want to err on the side of not honoring the privacy and civil liberties that we are all here to fight to keep.

Senator JOHNSON. I understand. Again, I appreciate your willingness to serve your Nation in this capacity. I think, your kind of background, your willingness to come from the private sector, a very lucrative job, I am sure, in the private sector, to really address this challenge is just really appreciated. Thank you.

Ms. SCHNECK. Thank you.

Senator COBURN. Uplifting.

Chairman CARPER. "Uplifting." That is what Dr. Coburn said. It is uplifting. Well, it is uplifting to have all of you before us, and, Ms. Dodson, nice to see you again. Thank you for your testimony. Mr. Caldwell, good to see you. Greg, thank you for joining us.

We are going to have to run and vote. We are running out of time, and they will not hold the clocks for us. So thank you all. There are going to be some questions, followup questions that you will be receiving subsequent to this hearing, and we just ask that you respond to those.

Chairman CARPER. And we look forward to an ongoing conversation. This has been a very encouraging panel, so thanks so much. And we should be reconvening around noon.

[Recess.]

We are going to reconvene now. I want to thank everybody for their patience and for waiting for us. When Dr. Coburn and I are the leaders of the Senate, we will not schedule these votes and interrupt our hearings. But we appreciate your patience and appreciate your being here with us.

Our first witness is a familiar-looking person. I think I have seen her before, Dr. Coburn. Elayne Starkey is our chief security officer (CSO) for the State of Delaware where she is responsible for the enterprise-wide protection of information assets from high-consequence events. Ms. Starkey is also the Chair of the Delaware Information Security Council and member of the Governor's Homeland Security Council. Before joining State government, Ms. Starkey spent 12 years in software engineering in the private sector, and, Tom, I just want you to know, for the 8 years that I served as Governor, most of those years I worked for this woman,

and it is great to see her again. We thank you for your service to our State.

Our next witness is David Velazquez, executive vice president and leader of power delivery business for Pepco Holdings Inc. (PHI). Previously Mr. Velazquez served as president and chief executive officer of Connective Energy. He serves on the boards of the Maryland Business Roundtable for Education, Southeastern Electric Exchange, the Trust for The National Mall, and the Smithsonian National Zoo Advisory Board. Welcome. Nice to see you.

Doug Johnson is vice chairman of the Federal Services Sector Coordinating Council, which advises the Federal bank regulatory agencies on homeland security and critical infrastructure protection issues. Mr. Johnson also serves as vice president and senior advisor of risk management policy, at the American Bankers Association (ABA), where he leads enterprise risk, physical and cybersecurity, business continuity and resiliency policy, and fraud deterrence. I understand you are also a member of the Financial Services Information Sharing and Analysis Center. Is that right?

Mr. JOHNSON. I am.

Chairman CARPER. OK. A private corporation that works with the government to provide the financial sector with cyber and physical threat and vulnerability information as part of our Nation's homeland security efforts.

A final witness, saving the best for last, the final witness is Steven Chabinsky, senior vice president of legal affairs, general counsel, and chief risk officer for CrowdStrike, a big data security technology firm specializing in continuous threat detection, cyber intelligence, and computer incident response. He also serves as an adjunct faculty member of the George Washington University and is a cyber columnist for Security Magazine. Before joining CrowdStrike, Mr. Chabinsky had a distinguished career with the government culminating in his service as Deputy Assistant Director of the FBI's Cyber Division.

A big thanks to all of you for coming, for your testimonies, and for your patience with us today.

Elayne, would you please proceed? Your entire statement will be made part of the record. You can summarize as you see fit.

TESTIMONY OF ELAYNE M. STARKEY,[1] CHIEF SECURITY OFFICER, DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION

Ms. STARKEY. Good afternoon, Senator Carper, Ranking Member Coburn. Thank you for the opportunity to be here at the hearing today.

As the chief security officer for the State of Delaware, I can report that we are combatting a greater number of cyber attacks than ever before. State governments not only host volumes of sensitive data about our citizens, we use the Internet to deliver vital services, and ensure our first responders can access the data they need in crisis situations. State government IT systems are a vital component of the Nation's critical infrastructure.

[1] The prepared statement of Ms. Starkey appears in the Appendix on page 85.

Today, with this testimony, I want to provide the Committee information on the value of public-private partnerships, as I see it from where I sit. Cyber threats know no borders, and in our interconnected world where all levels of government work with each other and work with private sector partners and citizens, the only defense is a multi-sector approach. I view these partnerships as a critical component of the Delaware Information Security Program, and I am eager to give you very specific examples of what is working in my State.

We have been partnering with the U.S. Department of Homeland Security since our program started back in 2004, and over the years, our incident response capabilities have improved significantly by partnering and participating in their Cyber Storm Exercises. We have advanced our capabilities, thanks to applying funding from the Homeland Security Preparedness Grant Program, and we have used this money for a variety of different things, including annual employee awareness training, e-mail phishing simulations, technical training, and I am most grateful to have received approval for this funding.

Delaware, however, is an exception. In contrast, most of my peers in other States report limited success in competing with traditional emergency responders for just a small share of those grant funds. I urge Congress to carve out a portion of this funding for States to use exclusively on cybersecurity initiatives.

One of the things I am most proud of is Delaware's effective outreach and collaboration with local governments and other critical infrastructure providers. We were delighted to be selected to participate in the Community Cyber Security Maturity Model, run by the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio. This program has resulted in training at all levels, and exercises, and seminars. In fact, our next event is a statewide cybersecurity conference on May 6. This is a day-long education workshop where we will bring together State and local government, law enforcement, military, higher education, health care, and other critical infrastructure providers.

Cyber awareness and education and training have been the cornerstones of Delaware's program ever since we got started. Our campaign is very active throughout the year. But in October, as part of National Cybersecurity Awareness Month, we racheted up the program with TV and radio advertising, and even wrapping a Delaware Transit bus with an eye-popping cybersecurity message. In the testimony that I provided,[1] if you cannot imagine what a wrapped cybersecurity bus looks like, there are some pictures in the testimony that I provided. This literally has become a moving billboard up and down the State, carrying the Internet safety message to 50,000 motorists each day.

We are unable to use State funding to do projects like that, so that is why I am so thankful to Verizon. Verizon's support of this program has been unwavering. We could not have done many of these initiatives without the financial support from the Verizon Foundation and the incredible volunteer support from Verizon employees as we go out into Delaware elementary schools and present

[1] The pictures submitted by Ms. Starkey appear in the Appendix on page 91.

on Internet safety. We have reached 25,000 fourth graders over the last 7 years thanks to this wonderful partnership that we have with Verizon.

Cybersecurity works best when people have an understanding of the risks and the threats, so I am especially appreciative of our strong partnership and collaboration with the Multi-State Information Sharing and Analysis Center (MS–ISAC) and the National Association of Chief Information Officers.

My final partnership example is with higher education. Five years ago, a team of people came together, and we discovered we all had the same passion. We had a passion for nurturing the next generation of cybersecurity professionals, and today that team includes all Delaware universities and colleges. And together with the Council on Cybersecurity and SANS Institute, we are planning our 5th annual U.S. Cyber Challenge summer camp. It is a weeklong, intensive training filled with specialized speakers intended to reduce the shortage in the cyber workforce.

So, in conclusion, my compliments to NIST and DHS and all the stakeholders that worked together to develop the Cybersecurity Framework. It is valuable to State governments. It is valuable to reference a core set of activities to mitigate against attacks on our systems. For those of us that have established security programs, the framework will not introduce major changes for us. Rather, the framework offers valuable risk management guidance and is complementary to our Exercise and Incident Response Program. I endorse the framework as an excellent first step; however, it is important to stress it is the beginning and it is not the end. My hope is that future versions are going to include incentives to adopt the framework and strive for continuous reduction of the cyber risk.

This is a complex issue. We have a long road ahead of us to making our Nation's systems more secure. It is a journey, and it is a race with no finish line. There is no single solution; there is no silver bullet. I compliment you for holding hearings such as these. I ask Congress to continue to work with States to identify ways to protect our Nation's information assets and provide funding opportunities for State government cybersecurity.

Thank you.

Chairman CARPER. Elayne, thank you so much. Great to see you here, and thank you for joining us.

Steven Chabinsky, please proceed.

TESTIMONY OF STEVEN R. CHABINSKY,[1] CHIEF RISK OFFICER, CROWDSTRIKE, INC. (TESTIFYING IN HIS PERSONAL CAPACITY)

Mr. CHABINSKY. Thank you. Good afternoon, Chairman Carper, Ranking Member Coburn. I am pleased to appear before you today to discuss cybersecurity public-private partnerships.

First, I would like to discuss the Cybersecurity Framework. Senator Rockefeller had proclaimed last year that NIST is the "jewel of the Federal Government." I agree. I especially commend NIST for having engaged with over 3,000 individuals and organizations on the framework. In doing so, NIST established a true public-pri-

[1] The prepared statement of Mr. Chabinsky appears in the Appendix on page 93.

vate partnership. I would also note that the Cybersecurity Framework is written in such a straightforward manner and so concisely that it should be required reading for every corporate officer and director.

I have no doubt that, if implemented, it would improve our critical infrastructure cybersecurity. But having improved security is not the same thing as having adequate security. And in my professional opinion, the strategy we are pursuing to include the NIST framework will not result in adequate security of our critical infrastructure and for our country.

Regardless of how vigorously industry applies risk management principles, there simply is no chance the private sector can consistently withstand intrusion attempts from foreign military units and intelligence services or even, for that matter, from transnational organized crime. As a result, improving our security posture requires that we reconsider our efforts rather than simply redouble them.

We must ensure that our cybersecurity strategies focus greater attention not on preventing all intrusions but on more quickly detecting them and mitigating harm while in parallel—and this is the significant part—identifying, locating, and penalizing bad actors. Doing so also would align our cybersecurity efforts with the security strategies we successfully use every day in the physical world.

In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, and depending upon the type of business, those locked doors and windows will be of varying strength and expense. Still, we do not spend an endless amount of resources seeking to cutoff every possible point of entry against those who might dig holes underground or parachute onto the roof.

Instead, to counter determined adversaries, we ultimately concede that they can gain unlawful entry. So we shift our focus. We might hire armed guards. More often we get security systems that have alarms for instant detection and video cameras to capture attribution. None of these make the facility any stronger or less penetrable; rather, in the physical world, guards, alarms, and cameras essentially declare to the bad guy, "It is no longer about us. Now it is about you."

When a monitoring company is alerted that a door was broken into at 3 in the morning, it calls the police to respond. It does not call the locksmith. And as a result, most would-be intruders are deterred from acting in the first place.

It is surprising then and suggests a larger strategic problem that, in the world of cyber, when the intrusion detection system goes off, the response has been to blame the victim time and again and to demand that they prevent it from happening again.

The goal then becomes one of ridding the network of malware rather than of finding and deterring the attackers. I believe that this single-minded focus of preventing or cleaning up after an intrusion is grossly misplaced.

Consider the scene in "The Godfather" movie of waking up to find a horse's head in your bed. That is no time to wonder how you are going to clean it up. Rather, the obvious questions are: Who did it? What are they after? Are they coming back? And what will it take to stop them or change their mind? It is threat deterrence, not

vulnerability mitigation, that effects security in the physical world every day.

Making matters worse, as industry and government agencies continue to spend greater resources on vulnerability mitigation, we find ourselves facing the problems of diminishing economic returns and perhaps even negative returns. With respect to diminishing returns, imagine trying to protect a building by spending millions of dollars on a 20-foot brick wall. Meanwhile, an adversary can go to a hardware store and for less than $100 buy a 30-foot ladder. That is happening every day in cyber where defenses are expensive and malware is cheap.

Far worse, though, is the concept of negative returns in which well-intentioned efforts actually make the problem worse. Consider our brick wall again. What if instead of buying a ladder the adversary decides to use a life-threatening explosive to bring down the wall? This is not dissimilar from our current defensive cyber strategy, which has had the unintended consequence of proliferating a greater quantity and quality of attack methods, thereby escalating the problem and placing more of our infrastructure at greater risk.

We can and must do better. It is time to refocus our public-private partnerships on developing the technologies and policies necessary to achieve the level of hacker detection, attribution, and punitive response that is necessary to reduce the threat. By doing so, businesses and consumers are far more likely to benefit from improved, sustained cybersecurity and at lower costs.

Thank you for the opportunity to testify today. I would be very happy to answer any questions you may have.

Chairman CARPER. Thank you, sir. We are very happy you are here, and thank you for that testimony.

Mr. Johnson, please.

TESTIMONY OF DOUG JOHNSON,[1] VICE CHAIRMAN, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

Mr. JOHNSON. Yes, Chairman Carper, Ranking Member Coburn, my name is Doug Johnson. I am vice president of risk management policy at the American Bankers Association. I am here today testifying in my capacity as the vice chairman of the Financial Services Sector Coordinating Council (FSSCC), and also in my capacity as a board member of the Financial Services Information Sharing and Analysis Center (FS–ISAC).

ABA is always proud of and committed to maintaining its leadership role in organizations such as these as we help to protect our Nation's critical infrastructure, and we feel that it is extremely important to do so as an association. The financial sector shares the Committee's commitment to strengthening the public-private partnership to reduce cyber risks to our Nation's critical infrastructure.

The nature and the frequency of cyber attacks against financial services and others sectors have focused a great deal of attention on whether our institutions, regardless of size, are properly prepared for such events and whether we are committing the appropriate level of resources to detect and defend against them. This is not a new exercise. The financial services sector continuously as-

[1] The prepared statement of Mr. Johnson appears in the Appendix on page 103.

sesses and refines our preparedness to detect and to respond to future attacks and actively engage our government partners in this process. These efforts build on a longstanding, collaborative imperative for the financial sector to protect institutions and customers from physical and cyber events. A significant protection infrastructure, in partnership with government, exists, and the FSSCC and the FS–ISAC obviously play vital roles in the process.

For the FSSCC, much of 2013 and now 2014 was and has been dedicated to responding to the administration's Executive Order, and particularly regarding the development of NIST's Cybersecurity Framework. You have heard a lot of compliments about the framework, and we share in that assessment. Our sector is supportive of the administration's and NIST's efforts in this regard to build a voluntary framework and will remain engaged as we migrate into what is really the all-important implementation phase of the framework.

Our government partners are many. Our partnership with DHS is really extremely important. Of particular note is DHS' assistance. The FS–ISAC is now the third sector which is participating in the National Cybersecurity and Communications Integration Center. The collocation of sectors in the NCCIC is an extremely important component of our overall effort to build the trusted network between government and industry, and the only way to do that, frankly, is to have an ability to really share information in very much of a trusted network, which requires individuals really to have that trusted ability to communicate with each other. And the NCCIC is a prime example of how the co-location of subject matter experts across the public and private sector can build that model. That enhances the ability both to protect our critical infrastructure and to build that trust.

The FS–ISAC also works very closely with other critical infrastructure sectors through the National Council of ISACs where our cross-sector cooperation and coordination for the FSSCC occurs through the Partnership for Critical Infrastructure Security (PCIS) Cross-Sector Council. The 20 sectors and the subsectors that really comprise the PCIS Cross-Sector Council are unanimously in support of it remaining the mechanism to engage DHS on our joint critical infrastructure protection mission. We look forward to working with DHS in a manner consistent with the National Infrastructure Protection Plan in that regard.

Through the FS–ISAC and the sector, our sector is committed to working collaboratively with NIST to further improve the framework and our Nation's overall cybersecurity posture. In my written testimony, I have offered a number of recommendations to meet our mutual goals, including: encouraging the development of sector-specific approaches to the framework; facilitating automated information sharing; clarifying liability protections for the sharing of information; fostering the growth of the existing ISACs and encouraging the development of additional models similar to that in other sectors that might not currently be deemed critical infrastructure protection; leveraging existing audit and examination processes when implementing the framework to the greatest extent possible; creating incentives that are tailored to address specific market gaps and letting the market make the determination as to whether

or not they can fill those gaps independent of government; and, last, fostering research and development and workforce creation is always very important, as you have heard others speak of today.

Thank you for holding this important hearing. Financial services companies do make cybersecurity a top priority. We look forward to continuing to work with you toward our mutual goal, and at this point I would be willing to take any questions.

Thank you.

Chairman CARPER. Thank you, Mr. Johnson.

And our last witness, Mr. Velazquez, please proceed. Good to see you.

TESTIMONY OF DAVID VELAZQUEZ,[1] EXECUTIVE VICE PRESIDENT FOR POWER DELIVERY, PEPCO HOLDINGS, INC.

Mr. VELAZQUEZ. Thank you, Chairman Carper, Ranking Member Coburn. I am Dave Velazquez, and I have the privilege of serving as executive vice president of power delivery for Pepco Holdings Inc. (PHI). We are an electric utility that serves about 2 million customers in the Mid-Atlantic area, including here in Washington, DC. It is my pleasure to appear before you today to discuss an issue of fundamental significance to our industry, the electric utility sector: the public-private partnerships to advance the security of our electric grid.

As the utility power in the Nation's capital, PHI has been actively engaged in cybersecurity protection and in the advancement of national cybersecurity regulations and legislation. In addition to Washington, we serve customers in four other jurisdictions. The thought that each of these jurisdictions could develop its own Cybersecurity Framework and protocols becomes quite daunting for us. That is why we believe Federal legislation is necessary, and we commend the work of this Committee and others in the House and Senate, the work that has been toward that goal.

We were very active in the public information gathering sessions led by NIST to develop the framework. We found that process to be very collaborative and respectful of the work that the electric utility sector and our regulators had already done.

PHI has pledged to be among the first utilities to work with DHS and the Department of Energy (DOE) to apply that framework to our operations. This self-assessment process is ongoing, but to be truly resonant with our regulators, PHI believes it should include some form of standardized third-party verification.

The framework is not, however, the first example of a public-private partnership for grid security. There are a number of others in which PHI is active. Critical Infrastructure Protection (CIP) standards are mandatory for all owners and operators of bulk power system assets, and they are enforceable by the Federal Energy Regulatory Commission (FERC). In this way, the CIP standards ensure basic network hygiene and baseline levels of security for the grid.

The NCCIC serves as a centralized location where cybersecurity operational elements are coordinated and integrated. NCCIC partners include the Federal agencies, State and local governments, the private sector, and international entities. PHI is in the process of

[1] The prepared statement of Mr. Velazquez appears in the Appendix on page 113.

obtaining the clearances needed to maintain a seat on the NCCIC floor.

The Electricity Subsector Coordinating Council, which is made up of utility and trade association leaders and government executives, has focused its efforts on three areas of industry-government collaboration: incident response, information flow, and tools and technology.

PHI is also an active participant in the ICS–CERT, a program that provides vulnerability information regarding industry control systems.

While the NCCIC, Electricity Subsector Coordinating Council (ESCC), and Industrial Control Systems Cyber Emergency Response System (ICS–CERT) are industry-wide initiatives, there are also opportunities for individual utilities to apply federally developed threat detection technologies. Though I am not at liberty to discuss the details of these threat detection programs, I can say that PHI has been afforded the opportunity to participate in Federal security technology applications that allow both temporary and also permanent real-time, machine-to-machine threat detection.

Additionally, last November the North American Electric Reliability Corporation (NERC) conducted Grid-Ex II, a 2-day cyber and physical security and incident response exercise in which more than 165 industry and governmental organizations participated. One of the key learnings from the exercise was the need for clearer protocols to coordinate governmental roles in the physical defense of privately held critical infrastructure.

Though these existing partnerships are impactful, there are some open issues that exist. For instance, though the federally administered technology programs in which a number of the utilities participate offer some threat information sharing capability, in the absence of Federal legislation much is left undefined with regard to data privacy and also liability associated with the bi-directional threat information sharing. Similarly, forums exist for event response coordination. Without explicit authorization, these forums may not resolve all the jurisdictional issues. And, very importantly, we must have clear protocols for industry-government event response before an event occurs. Finally, some assurance of prompt and reasonable recovery of cybersecurity investments will be imperative.

Today our regulators seem willing to acknowledge the value of the investments we are making in cybersecurity. However, as the threat continues to become more sophisticated, our investments will likely rise pretty rapidly, and some systemized form of prompt cost recovery would facilitate our capacity to grow our expertise.

In summary, PHI has been very active in and benefited greatly from the growing array of opportunities to partner with Federal, State, and local authorities. Public-private partnerships have improved cyber threat detection and cyber and physical event preparation and response coordination. However, more can be done.

In particular, some issues still needing attention include real-time and actionable threat information sharing, liability protection, event response protocols and systemized cost recovery. We look forward to continuing to work with the administration, this Com-

mittee, and your colleagues in the House and Senate to advance legislation to address these open issues.

Thank you.

Chairman CARPER. David, thank you very much.

Dr. Coburn has to be off to another meeting, and he is going to ask some questions. I am going to step out and take a phone call and then come right back and continue, and we will wrap up a little bit after 1. Dr. Coburn.

Senator COBURN. Thank you, Mr. Chairman.

Mr. Chabinsky, I am really interested in your testimony because you have taken a track that nobody else has taken here other than Senator McCain in his questions that he asked earlier. And you have a lot of experience in terms of deterrence with your past history. I was wondering what the other panelists thought about what he said. You all talked about mitigation of vulnerabilities, and he is talking about deterrence—one of which is cheaper, one of which is more effective. Any comments about what Mr. Chabinsky had to say?

Mr. JOHNSON. Well, Senator, I would be glad to take a first shot at that. I think that what we saw during the denial-of-service attacks that we had over a period of over a year gave us a real understanding of the dynamics associated with that particular issue.

I will go back to anecdote that occurred in a conversation between Treasury and a series of bankers from New York that are not necessarily shy in a lot of cases. Basically during the height of the denial-of-service attacks, they were asking Treasury whether or not the denial-of-service attacks in and of themselves were part of the defensive strategy that we as a Nation were taking as it related to Iran. And I think that what that really brought to the fore is the jobs issue. Whose job is it to really take that so-called active defenses? And I think that in large part that is an area that is still to be determined, because clearly it is the expectation of industry that government has a role, a substantial role in that defense, and obviously when we are talking about issues such as "hack back," there has been a lot of controversy associated with the private sector taking those kind of roles. And, in fact, it is illegal at this particular juncture to do so.

And I love Steve's analogies. He is always extremely good at them. But if you go back to the analogy of physical security, when the bank is robbed, it is not up to bank personnel to catch the robber.

Senator COBURN. Right. I agree.

Mr. JOHNSON. And so I think that while there is some substantial role that organizations have on the front end—and that role might migrate to some degree toward active defense—I think that we really have to be clear on what that line is.

Senator COBURN. But the key is that you can give the government attribution.

Mr. JOHNSON. Yes.

Senator COBURN. And the government by itself does not have that. So for it to act, we need to create a pathway so that that information on attribution can get to the government if the government is going to act on it.

Mr. JOHNSON. Right, and that is where the analogy still holds, because when you are talking about fiscal crime, essentially one of the first things the police are going to ask when the bank is robbed is, "What did the robber look like?"

Senator COBURN. Yes.

Mr. JOHNSON. And so I think that analogy still holds.

Senator COBURN. Mr. Velazquez.

Mr. VELAZQUEZ. I would just second Mr. Johnson's comments, and I think one of the critical pieces from a private-public partnership is being able to share that information in real time so that the government can take appropriate action.

Senator COBURN. Right, OK.

Mr. Chabinsky, are you familiar with the Deter Cyber Theft Act?

Mr. CHABINSKY. I am, Senator.

Senator COBURN. What do you think about that?

Mr. CHABINSKY. I think that that is exactly the right path that we need to be going down, which is threat deterrence, making sure that the recipients of illegally obtained intellectual property are not able to benefit from that to further actually impact our economy. Bad enough that our intellectual property is being stolen every day by foreign powers. Then to have the corporate recipients of those companies come back to our shores and unfairly compete against our industry is unconscionable. Thank you for introducing that.

Senator COBURN. Thank you.

Ms. Starkey, I thank you for your testimony and what you are doing in the State of Delaware. Maybe I have some bad news for you. The fact is that 3 or 4 years from now you are not going to be getting a penny from the Federal Government for what you are doing. And the question is, it is really not our role to do that. The taxpayers of Delaware ought to fund theirs. But our financial situation is going to be such—we are going back to trillion-dollar deficits even in a growing economy, 3 or 4 percent. So we are not going to be there.

So are you prepared as representative of the State of Delaware to do what you need to do without Federal money?

Ms. STARKEY. Yes, we recognize that, and we have seen the dwindling amounts that have been coming out of the Homeland Security Grant just over the last few years. That is the reason, that is exactly the reason why we pursued the partnership with the Verizon Foundation, to be able to continue the momentum that we had through non-government dollars, if you will. So we are fully prepared for that.

I cannot really speak on behalf of the budget writers in the Delaware State government.

Senator COBURN. I understand.

Ms. STARKEY. But it is something that we are paying attention to. We are alerting them that, you know, the threats keep going up, and there needs to be additional tools added to our toolkit to combat the threats all the time, and those tools—as has been pointed out here, those tools are expensive. It is very expensive to be secure.

Senator COBURN. But if we did more deterrence and less vulnerability mitigation, what we might see is less capability, because the

fact is if you take a bunch of smart people, no matter what you put on your network, they are going to eventually find a hole in it.

Now, we may respond to that. We may protect everybody else that was not attacked. But eventually, if they want to, the guys that want to rob the bank, they are going to rob the bank. They are going to do that. So Mr. Chabinsky's point is well made.

Mr. Chabinsky, you spent some time with the FBI. What resources now do we have at the FBI in terms of manpower in terms of going after these people versus what you think in your opinion we should have?

Mr. CHABINSKY. Thank you, Dr. Coburn, for the question. When you look at the FBI's resources, the FBI and the Secret Service both have concurrent jurisdiction over cyber crime, and the FBI has exclusive jurisdiction when the intrusions are nation state sponsored.

The FBI's manpower of agents that are exclusively focusing on intrusions is in the hundreds, not thousands of persons. And since this crime is international, one would then look to see what resources the FBI has to place special agents abroad, working with partners in other countries who actually want to work with us. And what we see is that those are able to be counted on both hands.

So we are looking at a problem that, on the defensive side, we are putting tens of billions of dollars into, and on the side that actually could help the private sector make those handoffs to the government to have threat deterrence, put these bad guys in jail, we are severely understaffing and underfunding that.

Making matters worse, when we look at the Presidential Executive Order, the Executive order is focused on steering some of those very investigative resources away from investigations and toward warning the private sector that it is under attack. So now you have a limited pool of resources that should be investigating the crime. Now they are spending all day actually warning victims. And we do not see anything in the Executive Order that functions get the private sector to provide information to law enforcement to work hand in glove to try to figure out who these bad guys are and to bring them to justice.

Senator COBURN. That is really important for us as we try to write a cyber bill.

I have a lot of other questions, but my time constraints will force me to put them in the record. Thank you.

Chairman CARPER. Let me ask a question for Elayne Starkey, for David, and for Mr. Johnson. OK? I think one of the interesting, maybe unique features of the framework that has been constructed is that it can apply equally to an energy company, a utility, a bank, even a State or local government. It is also scalable so that both small business and large business can take advantage of it. All of you have already touched on how you will be using the framework in your statements, but I would like to ask you to drill down on this issue just a little bit more. OK?

What can we do, not just this Committee, not just the Federal Government, but government and industry, maybe working together, to encourage more businesses to adopt the framework that has been produced? In particular, can you talk with us a little bit about what type of help you would like to see from the Department

of Homeland Security and other Federal agencies as you and your sectors work to implement the framework? Elayne, if you would start that off, I would appreciate it.

Ms. STARKEY. Sure. I am glad you asked the question. Business adoption of this, in particular small to medium-sized business, is absolutely critical to the success, in my opinion. The larger companies have established programs, and they have been paying attention to this for a long time. It is the small and medium-sized businesses that maybe do not know what they do not know, or just simply do not have the resources to throw at this problem.

It is a huge problem. It is an expensive problem. And, quite frankly, it does not increase or improve their bottom line by adding a lot of security defenses necessarily. So that is not an automatic.

So I think it is going to be critical in the next few months and years as we see how this is going to be rolled out and adopted by not just governments but by the private sector as well.

The second part to your question in terms of what DHS can do, certainly what our plans in Delaware are——

Chairman CARPER. And not just DHS, but other relevant Federal agencies, please.

Ms. STARKEY. OK, sure. In Delaware, we have had an established program now for a number of years based on the International Organization for Standardization (ISO) international standards and NIST standards, and they have served us incredibly well. We do not plan to change that because our whole framework is centered around those NIST and ISO standards. But what we are going to do and have started to do is to take this framework and overlay it with our current framework and identify where there are gaps and work to close those gaps.

So we will be anxious to see—we are following the rollout from DHS. I know there is a kickoff meeting tomorrow, actually, all morning tomorrow. We are fortunate because I know cyber resilience is a huge part of the rollout plan, and we have some success with that, because back in 2010 we invited DHS to come in and do a cyber resilience study for Delaware State government, and it was an incredibly valuable exercise for us. We got a lot of good feedback. They brought in folks from US–CERT, from Carnegie Mellon, as well as here in D.C., and they spent all day with us talking to a variety of different parts of my department and parts of State government. And I was so pleased to see that that cyber resilience program is part of their rollout strategy. So I am looking forward to that.

Chairman CARPER. That is good to hear.

Mr. Chabinsky, same question—or no, you are the one person that gets—— [Laughter.]

David.

Mr. VELAZQUEZ. Yes, I think first I would mention that I think with the NIST framework, the flexibility that has been built inherent in it, and as that flexibility continues and being respectful of other regulations that cover the different sectors, I think that is very helpful for the continued adoption and more people adopting it.

I think if there are incentives for participation, although I would note that, like most companies, the real incentive for participation

is our customers and providing them service. And I think if any business, if your customers lose confidence in your ability, you lose business. But beyond that, we had talked already about liability protection, I think could help spur some others adopting it. If there is a way to provide discounted terrorism insurance as a result of that, access to Federal technologies maybe that comes with that, and then as a regulated industry as well, support for timely recovery of the investments necessary to support it. All those I think would help.

Chairman CARPER. Good. That is helpful. Mr. Johnson.

Mr. JOHNSON. Yes, as you indicated, probably in financial services, we are already essentially at the highest tiers within the Cybersecurity Framework. And so the question becomes one of two things: What do financial institutions have to do associated with the framework? And then how can they leverage the framework in their environment to increase adoption?

I think one thing that I have seen in our institutions is they are largely doing what the framework is—they might call it different things in different places, but by and large, conceptually the manner in which the framework is devised, financial institutions by and large are doing that.

And so one of the things I think will be to our advantage is the ability to leverage this within our supply chain. We have heard talk of that in the earlier panel. I think it is really vital to be able to give those supply chain partners a mechanism to think about what cybersecurity should look like in their organization and to aspire toward various tiers, to aspire toward the next tier, if you will, and to have a path forward. And I think the framework gives them that in large degree. And so I think that will be helpful for not only the critical suppliers that we have that are by law supposed to be adhering to the same information security standards that we do as financial institutions, but also the less critical suppliers as well, because I do not know that, for instance, the air conditioning supplier to Target was felt to be a critical supplier but, nonetheless, I think what that points to is the need to have the entire environment have some higher level of cybersecurity. And I think the framework essentially enables you to do that.

From the standpoint of what government could do, sometimes I think it is helpful if government would set their children free, if you will. I think that NIST has a tendency to do that with standards and is looking to do that to some degree with the framework where—trying to find a home for the framework for implementation purposes, for instance. But I would think long and hard before I established legislative incentives before I see what the market can do in terms of incentives. I see insurance companies, for instance, already going into our financial institutions and asking how the institution is thinking about the Cybersecurity Framework. I see insurance associations that write those policies coming to us as financial institutions and rethinking how they might want to write those cybersecurity policies on the basis of the framework. And so I think some of that thinking is very important to lay the groundwork for where the gaps are from the standpoint of incentives, because I do not know that we know yet where those gaps are.

Liability has been spoken of as a particular gap, and I think that for one thing, liability means a lot of different things in terms of protection to a lot of different people. And I think that one of the things that we saw, going back from the denial-of-service attacks again, is the fact that, to some degree, the sharing of information was impeded by the potential for the use of that information to have unintended consequences. And by that I mean when you want to shut down, for instance, a set of Internet addresses or compel an Internet service provider to take a certain action that might actually harm some individuals that are innocent, what kind of protections does that particular company have associated with taking that action? Can they be subject to civil suits to the extent that someone is harmed in that environment?

So I think that is something that we need to potentially look at from the standpoint of liability protection, is the use of that data. And under what criteria should personally identifiable information, properly defined, be able to be utilized to the extent that a threat is imminent? To what extent are Internet protocol or Internet addresses personally identifiable information? Are they not? There is some uncertainty associated with that. So I think those are some things the government could certainly be able to do.

Chairman CARPER. Good. Well, those are all very helpful answers. Thank you.

One last question, and we will break and send you on your own, and I will go back to my day job. I had originally thought I would ask the same question of these three people. I am going to ask Mr. Chabinsky to join in on this question if you would like to as well. But failures in our critical infrastructure can, as we know, have cascading effects that ripple through our communities, our lives. For example, if the power goes out for an extended period of time, our communications, our transportation, our drinking water might all be negatively impacted in some way. Should something terrible happen like that—and it probably will—I am not so sure we have clearly defined the roles and the responsibilities of the Federal Government, States, and the private sector to respond.

Two questions, if I could. One, are you confident that you will know who to turn to for help if there is a major cyber incident that takes down some of our most critical infrastructure for an extended period of time? And the second question would be: Are there any roles and responsibilities that need to be more clearly defined in law so you know what to expect and from whom? Elayne, if you would like to take a shot at that?

Ms. STARKEY. Part one is extremely confident. I would like to think that I should not be in the job I am in if I was not confident in that. The reason I am so confident is because we practice. We simulate. We have held nine consecutive annual exercises involving examples like you just gave. They are simulations, granted. It is different when it is the real thing. But we pull together those folks. Not only am I confident of knowing who to contact, I am reasonably comfortable with what their response is going to be and what their readiness level is. So, that is what drills are all about. So definitely for part one.

Part two is additional roles and responsibilities. Yes, I think that comes out of every exercise, is areas for improvement, action items,

corrective action items, communication is always one that comes out in various channels that can always be improved, and we try to do that on an annual basis.

Chairman CARPER. OK. thanks.

Mr. Chabinsky, I do not know if you have a comment here, but if you do in response to either questions, please feel free.

Mr. CHABINSKY. I do appreciate the opportunity, Chairman Carper. From my time in government, I believe that the government actually is very well situated with specific discrete roles and responsibilities that it has communicated effectively to the private sector. The National Cyber Investigative Joint Task Force, for example, that is led by the FBI but includes DHS and other agencies, has a clear responsibility for organizing the investigative approach to find out who the bad guy is and to try to bring that to an end.

The Department of Homeland Security, both on the vulnerability mitigation side, has gone out to owners and operators and has provided on-the-ground assistance with mitigation efforts, and in the worst-case scenario, if FEMA were needed to be brought in under DHS for consequence management, I believe that those roles are actually quite well understood.

The issue that I pointed out in my written testimony, though, is I think there really has not been a very effective coordination in the area of emerging threats, and one of those threats that I wanted to bring to the attention of this Committee is the emerging threat of purposeful interference. Whether it is GPS signals or just regular communications jamming that could impact first responders, that is an area where there is currently no centralized place for reporting information, no central analysis of data that is coming off of purposeful interference events, and law enforcement not at this moment coordinating its response with education and technologies that would be necessary to quickly isolate and identify from where the interference events are coming. So I think that there are certainly areas to extend public-private partnership specifically focused on emerging threats.

Chairman CARPER. Good. Thank you.

Mr. Johnson, if you could be fairly brief, I have other people waiting for me, so I do not want to cut you off, but just be brief, if you will. And David as well.

Mr. JOHNSON. What Mr. Chabinsky said. [Laughter.]

Mr. VELAZQUEZ. The only thing I would add is we very much know who to turn to. Our concern is more in a major event having too many different agencies turning to us, and the coordination and the clear roles defined so that we do not have the FBI, DOE, DHS, and three other agencies showing up on our doorsteps all wanting the same thing. And I think tremendous advances have been made, and the Grid-Ex exercise pointed out some of those advances, but also pointed out the need to continue to define those roles more clearly.

Chairman CARPER. OK, great.

Mr. JOHNSON. I do think that the NCCIC provides an opportunity for collocation that can solve some of those problems as well. So that would be the comment that I would make, is try to find a way to really have security operations centers to effect the kind

of trusted network you need to really have the proper level of response in a lot of instances.

Chairman CARPER. All right. Thank you. Thanks for adding that.

We are in your debt for a lot of reasons: one, for the good work that you have done and continue to do with your lives; we are in debt to you for being here today and preparing for this testimony and giving it and responding to Dr. Coburn's questions in writing.

We will keep the record open for about 15 more days, until April 13 at 5 p.m., for the submission of statements and for questions for the record. If you get some questions, I would just ask that you respond to them promptly, and that will be much appreciated.

Again, great to see you all, and thank you so much for being a part of this. I apologize you had to wait. Sometimes we have to vote on things over on the floor, and we had about four of them today, and so it disrupted our hearing. But thank you for going with the flow.

Thanks, and with that we are adjourned.

[Whereupon, at 1:13 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Thomas R. Carper
Strengthening Public-Private Partnerships to Reduce Cyber Risk to our Nation's Critical Infrastructure
March 26, 2014

As prepared for delivery:

A little more than a year ago, President Obama signed an Executive Order which put into place a number of efforts intended to enhance our nation's cybersecurity. We are here today to see what kind of progress has been made in implementing the Order and to gather other ideas about better securing our critical infrastructure from cyber attacks.

Every day, sophisticated criminals, hackers, and even nation states are probing our government agencies, universities, major retailers and critical infrastructure.

They are looking for weak spots in our defenses. They want to exploit these weaknesses to cause disruptions, steal our personal information and trade secrets, or even worse, cause us physical harm.

While we have been able to hold off some of these cyber attacks, anyone who has examined this issue even casually will tell you that our adversaries are getting into our systems every day. Earlier this week, for instance, the Washington Post reported that Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked.

Still, we have made some significant progress over the last year. For example, DHS and other federal agencies have taken steps to share more timely and actionable cyber threat information with the private sector.

And I know in talking to many businesses that the cooperation between the federal government and industry on dealing with the cyber threat has gotten much better.

One of the most significant accomplishments over the last year though, was the release of a voluntary cybersecurity framework. This framework provides those who choose to implement it – whether they be government entities, utilities, or businesses large and small - with a common-but-flexible set of best practices and standards they can use to better secure their systems. I tend to think of the framework as a "blueprint" or "roadmap" for stronger cybersecurity.

The President's Executive Order called on the National Institute of Standards Technology, including Ms. Dodson here, to work hand-in-hand with industry to develop the framework. It is a living document, so NIST, working with industry, will continue to update the framework to include lessons learned and address the latest cyber threats.

From what I understand, the development of the framework ran very smoothly and the end result is a product that has been well-received by many stakeholders.

In fact, just last week in Delaware, I sat down with a group of cybersecurity experts at DuPont who were all extremely appreciative of the public-private collaboration that went

into developing the framework. To NIST and all the partners that worked on this framework together, I say 'Bravo Zulu.' But, I think we can all agree that we have not yet crossed the finish line.

Right now, many organizations across the nation are actively analyzing the framework to determine how they can use it and incorporate it into their own cyber practices. I commend those efforts, and I am pleased that we have several witnesses with us today who will share their thoughts on using the framework.

Naturally, not every company or state is ready to use the framework. Some may not even really understand what it is. To these organizations, I say, help is around the corner.

"Under the leadership of the very talented Dr. Phyllis Schneck, the Department of Homeland Security has launched a new voluntary program to assist organizations in adopting the framework.

This program will be incredibly important to the success of the framework. And we will be closely monitoring its progress to ensure it is providing the right tools and information to stakeholders. For instance, we need to make sure our nation's small and medium-sized businesses are getting the attention they need to really drill down on the framework.

At the end of the day, I think the question that we are all asking is whether or not the framework will help improve our nation's cybersecurity. While it might be too early to answer this key question, I do believe that the framework itself provides a much a much needed roadmap for companies that want to improve their cybersecurity. This is a great first step.

Of course, the framework will only be successful if companies actually use it – so it is time for industry to roll up their sleeves and put this roadmap to use. It makes business sense too. In the words of Dr. Pat Gallagher, the head of NIST and now Acting Deputy Secretary of Commerce, "good cyber security is good business."

When you consider the threat we are up against, however, I think we can all agree that there is much more that needs to be done. That is why I continue to believe that bipartisan legislation is the best long-term solution to address this growing threat. I have been working hard with my Ranking Member, Dr. Coburn, in an attempt to produce such legislation.

For example, I believe we need to modernize the way we protect our federal networks from cyber attacks.

We also need to clarify and strengthen the public-private partnership we want Department of Homeland Security and industry to have regarding cybersecurity.

We need to make information sharing easier so that companies can freely share best practices and threat information with each other, and with the federal government. Finally, we need continue to develop the next generation of cyber professionals and enhance our cyber research and development efforts right here at home.

Last week, I had the privilege of visiting a new cybersecurity class at the University of Delaware. I was incredibly impressed with the students and was even told that the class was "oversubscribed." That is a good problem to have.

Those students at the University of Delaware, they get it. They understand what cybersecurity means and how important it is for our economic and national security. Our friends with us today, they understand it too.

But for some other folks, this is just a hard issue to grasp.

It is my hope that the framework can jumpstart a new conversation about cybersecurity in our country. And it is my hope that we can come together as a nation – government and industry, Democrat and Republican – and work together to tackle this growing threat we face.

###

Opening Statement of Ranking Member Tom Coburn

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

As prepared for delivery:

Cyber threats are one of the most serious national security threats facing our nation. Nation-states and other adversaries continue to commit or condone cyber espionage against our businesses and citizens — stealing our intellectual property and sensitive business information. Some have called these attacks the greatest transfer of wealth in human history and one of the significant headwinds facing our economy. Cyber-crime is also a growing and serious problem — imposing significant costs on our citizens and our economy. I remain concerned about the potential acts of cyber-sabotage or terrorism against our nation's critical infrastructure from those who wish to do us physical harm and disrupt our way of life. How to address and mitigate these threats will be one of the biggest challenges facing our nation in the years ahead.

I appreciate the hard work of the officials at the National Institute for Science and Technology (NIST) and the Department of Homeland Security (DHS). Their dedication to public service is uplifting. Ms. Dodson, I applaud NIST for the good job you did developing the Cybersecurity Framework. You worked with the private sector, listened to their ideas, and developed a workable, flexible process that can have significant positive impact in the private sector.

Dr. Schneck, I am interested to hear more from you about the DHS's plans for working with the private sector and states to help them use this tool, as well as your plans to encourage its adoption. I am also interested to hear your plans to encourage better information sharing from and between government and the private sector. Information sharing is most important partnership we can form to help our businesses better defend their own networks.

More clarity is needed regarding the ultimate goal of Executive Order 13636 though; it should not be federal regulation of cybersecurity. The last thing that we need is a top-down regulatory model for cybersecurity. Let's be clear — Washington does not have all of the answers for cybersecurity. Even if it did, the Federal Government would struggle to manage or enforce rules for good cybersecurity practices. Each computer network is unique and computer networks are not well-suited to the inflexible, prescriptive, check-the-box approach of a regulatory regime. I worry that a mandatory cybersecurity framework would harm cybersecurity more than it helps — shifting resources from dealing with actual cybersecurity risk to regulatory compliance.

Consider the Federal Government's poor track record of securing its own networks. As I revealed in my report last month — *The Federal Government's Track Record on Cybersecurity and Critical Infrastructure*, which I will include in the record for this hearing — many agencies are still failing to practice the basic cyber hygiene necessary to protect their computer networks and systems. Even the Department of Homeland Security has trouble securing its networks. For example, DHS is one of several federal departments and agencies that continues to run Windows XP on some computers, which Microsoft will stop issuing patches and software updates for early

next month. Systems running Windows XP will become ripe targets for hackers once Microsoft stops supporting those systems. It is simply irresponsible to run such unsecure operating systems on critical systems and government networks.

With the Federal Government unable to maintain its own cybersecurity, why should the private sector trust it to be a competent manager or regulator? Let me quote the November 2013 report of the *President's Council of Advisors on Science and Technology,* which was prepared by some of our top experts in science and technology and released by the White House:

> *The Federal Government rarely follows accepted best practices. It needs to lead by example and accelerate its effort to make routine cyber-attacks more difficult by implementing best practices for its own systems.*[1]

The Council's first recommendation was to phase out the use of unsupported and insecure operating systems, such as Windows XP, in favor of modern systems within two years. If the Federal Government is to be a trusted and effective partner in cybersecurity, we need to lead by example and get our own house in order first.

We also need to do a better job with our programs working with the private sector. I am pleased to have Mr. Stephen Caldwell here from GAO to testify today. He will review the Department of Homeland Security's track record working with critical infrastructure sectors. Too often the Department has struggled to implement programs like the Chemical Facility Anti-Terrorism Standards (CFATS) program and information sharing with the private sector. My hope is that DHS experts will learn from their past mistakes and GAO's analyses to become more successful in rolling out programs through better consultation with the private sector.

We also need to question whether the Federal Government's current approach to cybersecurity is the right one. Rather than just focusing on vulnerability mitigation — putting more locks on the doors to our networks — we need to be thinking about deterrence — disincentivizing bad actors from trying to break through those doors in the first place. A determined adversary like a nation state is going to be able to get into our networks regardless of our defenses. As Suzanne Spaulding, who now leads federal cybersecurity programs like Einstein and Continuous Diagnostics and Mitigation as DHS's Under Secretary for National Protection and Programs, once wrote, "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth."[2] I agree.

We need to be changing the cost benefit analysis of our adversaries, so they think twice about whether attacking our networks. There is bipartisan interest, including from some members on this Committee in applying deterrence as a strategy through bills like the Deter Cyber Theft Act. I am pleased to have Mr. Steve Chabinsky — formerly of the FBI — here with us today on our

---

[1] EXECUTIVE OFFICE OF THE PRESIDENT, PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: IMMEDIATE OPPORTUNITIES FOR STRENGTHENING THE NATION'S CYBERSECURITY (November 2013), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf.

[2] Suzanne E. Spaulding, *No More Secrets: Then What?*, THE BLOG, HUFFINGTON POST (June 24, 2010, 10:55), http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html.

second panel. He has been on the front lines of the cyber fight since the 1990s and can speak to this issue, whether we are following the right strategy, and what more can be done.

In closing, there is no question that cybersecurity is an increasing problem for our nation, and it is only getting worse. It is also true that when Congress tries to write big bills, they often go nowhere; or worse, they pass and only exacerbate the nation's problems. One area where I do think we can focus is fixing cybersecurity within the Federal Government. If the Federal Government is to be an effective and respected partner with the private sector, it needs to start with improving its own cybersecurity.

I thank you and look forward to your testimonies.

Testimony of

NPPD Deputy Under Secretary for Cybersecurity

Phyllis Schneck

Before the

Senate Homeland Security and Governmental Affairs Committee

Regarding

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"

March 26, 2014

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) work to improve the cybersecurity of critical infrastructure. We view cybersecurity as key to the larger goal of infrastructure security and resilience. Therefore, DHS takes a holistic, cross-sector view of cybersecurity as a risk management decision that needs to be part of the executive discussion in organizations of all sizes across government and industry. America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards, including attacks via the Internet. In this spirit, today I will speak to our cybersecurity mission, implementation of Executive Order (EO) 13636 and delivery of our Critical Infrastructure Cyber Community (C^3, pronounced "C-Cubed") Voluntary Program, which promote cybersecurity for critical infrastructure to enhance their shared security and resilience.

DHS Vision for Cybersecurity

DHS continues to strengthen trust and public confidence in the Department through the foundations of partnership, transparency, and protections for privacy and civil liberties, which is built in to all that we do. Our Department is the lead civilian agency responsible for coordinating the national protection, prevention, mitigation, and recovery from cyber incidents across civilian government, state, local, tribal, territorial (SLTT) and private sector entities of all sizes. DHS leverages our interagency and industry partnerships as well as the breadth of our cyber capabilities extending from NPPD, Immigration and Customs Enforcement's Homeland Security Investigations, U.S. Coast Guard and U.S. Secret Service, to make our National Cybersecurity and Communications and Integration Center (NCCIC) the source of a "weather map" for global cyber indicators and activity.

We are working to further enable the NCCIC to receive information at "machine speed."[1] This new capability will begin to enable networks to be more self-healing, as they use mathematics and analytics to mimic restorative processes that occur biologically. Ultimately, this will enable us and our partners to better recognize and block threats before they reach their targets, thus deflating the goals for success of cyber adversaries and taking botnet response from hours to seconds in certain cases. We are working with the DHS Science & Technology Directorate in many areas to develop and support these capabilities for NCCIC. The science of decision-making is about seeing enough behavior to differentiate the good from the bad, and that comes from the collective information of industry and government. That is voluntarily provided to us because of underlying trust.

We can increase the availability of information flow through stakeholder engagement, constant trust-building to optimize the information shared voluntarily and better use of current authorities. At the

[1] Automatically sending and receiving cyber information as it is consumed and augmented based on current threat conditions, creating a process of automated learning that emulates a human immune system and gets smarter as it is exposed to new threats.

core of this effort, we also must continue to ensure that privacy and civil liberties protections are baked in to everything we do and we do this primarily by focusing on the sharing of cyber threat information that is non-attributable and anonymized to the greatest extent feasible.

To develop a National Oceanic and Atmospheric Administration-like capability in dynamic data aggregation to a "weather map" will require a significant leap forward from our current efforts sharing information at human speeds with mostly manual processes. DHS seeks machine-speed information sharing with a broad set of partners, which will require an internal data management system that provides real-time situational awareness from which people and tools can extract information. Some of this effort is currently being built in our Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII™) programs that we have begun offering as a free method for machine-to-machine sharing of cyber threat indicators to others in the government and private sector.

The programs that DHS has created provide a sound foundation for the above vision. DHS's extensive visibility into attacks on government networks must be fully leveraged to protect all government networks as well as our critical infrastructure and local entities, in a way that is consistent with our laws while preserving the privacy and individual rights of those we protect. We continue to believe legislation providing a single clear expression of DHS cybersecurity authority would greatly enhance and speed up the Department's ability to engage with affected entities during a major cyber incident and dramatically improve the cybersecurity posture of federal agencies and critical infrastructure.

Implementing Presidential Directives

In February 2013, the President signed EO 13636 on Improving Cybersecurity Critical Infrastructure and Presidential Policy Directive (PPD)-21 on Critical Infrastructure Security and Resilience. These presidential policy documents direct Federal agencies to use their existing authorities and increase partnership with the private sector to provide better protection for the computer systems and networks that are critical to our national and economic security. Critical infrastructure security and resilience requires partnership between public, private, and non-profit sectors, and a clear understanding of the risks we face. To that end, EO 13636 and PPD-21 emphasizes an integrated approach to promoting critical infrastructure cybersecurity. DHS's role is to bring together all stakeholders—government officials and business leaders, security professionals and infrastructure owners and operators—to facilitate information-sharing and support adoption of standards and best practices to reduce and manage cyber risk.

Strengthening the security and resilience of critical infrastructure against growing and evolving cyber risks requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the nation's critical cyber and communications

networks and to reduce adverse impacts on critical network systems. Thus, to implement the EO and PPD 21, the Federal Government has actively sought the collaboration, input and engagement of all our partners.

Cybersecurity Framework & Voluntary Program

EO 13636 directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework, based on standards and industry best practices for improving cybersecurity and promoting cyber risk management. The EO also directed DHS to establish a voluntary program for critical infrastructure cybersecurity, to serve as a Federal coordination point for cybersecurity resources and support increased cyber resilience by promoting use of the Framework. The C^3 Voluntary Program is an innovative public-private partnership that is critical to DHS. DHS leads this program as part of its mission of continuing outreach and collaboration with the civilian federal government, state, local, tribal and territorial governments and private sector. C^3 helps to align critical infrastructure owners and operators with existing resources that will assist their efforts to manage their cyber risks, including through use of the Framework. The C^3 Voluntary Program also facilitates forums for knowledge sharing and collaboration. It provides access to free and readily available technical assistance, tools, and resources to strengthen capabilities to manage cyber risks, and opportunities to exchange opinions with peers and other partners in the critical infrastructure community.

As an example, one resource in the C^3 Voluntary Program is the Cyber Resilience Review, a no-cost assessment tool that helps organizations of all sizes review the strengths and weaknesses of their cyber systems through a self or facilitated risk-assessment. DHS has already facilitated more than three hundred of these assessments, helping organizations identify and address weaknesses in their systems.

Support to Partners

State, local, territorial, and tribal (SLTT) governments are some of our frontline stakeholders and can serve as a force multiplier in the national effort to protect critical infrastructure. DHS works with these partners, including through SLTT associations such as the National Association of State CIOs and the National Governors Association, to both strengthen the security and resilience of their critical networks, and better protect the public from constantly evolving cyber threats. However, due to challenging budgetary environments, states and territories often lack the resources to obtain advanced security tools. To help address this critical gap, DHS recently forged a cooperative agreement with the Center for Internet Security (CIS) Multi-State Information Sharing and Analysis Center to provide state-of-the-art managed security services to states and territories in conjunction with their use of the NIST Cybersecurity Framework. As part of this agreement, CIS will provide Managed Security Services, funded by DHS, to states and territories in 2014. These

services include intrusion detection, intrusion prevention, netflow analysis and firewall monitoring – all things that support critical elements of the Framework. While states and territories must retain full authority and ownership over their networks, and manage those networks commensurate with the risk, these services, and the use of the Framework are critical tools to assist reaching that goal.

DHS is also working to promote use of the Cybersecurity Framework to other groups of entities, such as small and medium businesses (SMB). These entities store significant amounts of sensitive data, from customer information to critical intellectual property, yet may lack the education or resources to properly protect this data or critical systems they manage. Under the C^3 Voluntary Program, the Department has issued a request for information (RFI) to ask industry about the market of affordable cybersecurity solutions and the specific challenges that SMB may face in managing cyber risk. We are encouraged by the initial response from many industry stakeholders and look forward to continuing this effort.

Incentivizing Cybersecurity

While the strongest motivation for use of the Cybersecurity Framework is increased security and resilience of an entity's networks, EO 13636 also directed DHS, along with the Departments of Treasury and Commerce, to evaluate incentives to further encourage participation in the DHS Voluntary Program. This work led to the identification of eight incentive areas that are being analyzed among Federal departments and agencies as well as industry stakeholders. They include cybersecurity insurance, grants, process preferences, liability limitation, streamlined regulations, public recognition, cost recovery for regulated industries, and cybersecurity research and development. Some of the recommended areas are direct incentives, while others are indirect such as cyber insurance. Also, some can be implemented with current authorities or as part of the C^3 Voluntary Program, while others, such as liability limitation, may require legislative action.

Based on feedback from stakeholders, agencies have further defined the scope and path forward for each area. For example, based on further analysis, the cost recovery incentive area has been revised to "support for prudent cybersecurity investments and opportunities for utilities".

Independent of added incentives, DHS hopes that our partners in critical infrastructure will consider use of the Framework as an effective way to manage cyber risks consistent with their business needs. These incentives may provide helpful and positive reasons encouraging participation of in the C^3 Voluntary Program and use of the Framework to manage cyber risks.

Continuing Need for Congressional Support

While securing cyberspace has been identified as a core DHS mission since the 2010 QHSR, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical

infrastructure which takes into account risks across the spectrum. In a time of constrained resources, we must ensure that our efforts achieve the highest level of security as efficiently as possible. To achieve success, however, it is vital that funding requested in the President's budget for NPPD be maintained and preserved, not only for cybersecurity programs but also those that tie in physical world security with networked systems. The Committee has always been a supportive partner in our cybersecurity efforts, including the recent confirmation of NPPD's Under Secretary Suzanne Spaulding, and I would ask that now more than ever, this support remains firm.

Furthermore, we must attract the best and brightest to DHS. We have an urgent and exciting mission. I left the private sector because I believe in what DHS can do with the current leadership in NPPD and at the top of our Department. What Government cannot always pay in money, I believe we can offer in mission and the opportunity to solve a giant but exciting problem that involves computers, people, policy and our way of life. I have visited universities with our Secretary and spoken at several student events. There is eager talent out there, and it is ours to lose. Once we attract that talent, we need to be able to hire those people and to improve our processes to not foil our recruitment efforts.

While the Nation's dependence on cyber infrastructure has grown exponentially since the Department's founding, the Administration believes the Department's statutory authorities have not kept pace with evolving technologies and reliance on cyberspace by Federal agencies and critical infrastructure. To enable DHS and other agencies to more effectively and efficiently carry out their existing responsibilities, legislative action is necessary. We ask that such legislation, aligned in principle with the Administration's 2011 legislative proposal, modernize FISMA and reflect the existing DHS role in agencies' Federal network information security policies as well as clarify existing operational responsibilities for DHS in cybersecurity.

Conclusion

Thank you for the opportunity to share with you some of our ongoing work as well as our vision for future capabilities. Our mission to secure critical infrastructure requires continuous collaboration with other Federal agencies, SLTT and private sector partners, and DHS is deeply committed to further this mission.

We will continue to work with our public and private partners to strengthen the security and resilience of our critical infrastructure. We thank the Committee for their support and look forward to building a more secure and resilient future in which cyberspace remains a catalyst for innovation, growth, and prosperity.

Testimony of

Donna F. Dodson
Chief Cybersecurity Advisor
National Institute of Standards and Technology
United States Department of Commerce

Before the United States Senate
Committee on Homeland Security and Governmental Affairs

"*Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure*"

March 26, 2014

Introduction

Chairman Carper, Ranking Member Coburn and Members of the Committee, I am Donna F. Dodson, the Chief Cybersecurity Advisor working in the Information Technology Laboratory (ITL) in the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for this opportunity to testify today on NIST's responsibilities under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" and our work through public-private partnerships in the area of cybersecurity.

Background

Let me begin with a few words on NIST itself: NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. Our work in addressing technical challenges related to national priorities has ranged from projects in the smart grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In cybersecurity, we have worked with federal agencies, industry, and academia dating back to the mid-1970s to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with this mission, NIST actively engages with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the federal government and critical infrastructure companies.

The Role of NIST in Executive Order 13636

NIST has spent the last year working to convene Critical Infrastructure sectors to build a Cybersecurity Framework as part of Executive Order 13636. Version 1.0 of the Framework was released on February 12, 2014, along with a Roadmap for future NIST work in support of this effort.

The Executive Order asked NIST to develop a Framework – a collection of industry standards, process, and best practices – that could be leveraged more broadly to help companies manage their cybersecurity risk. NIST's approach was to work with stakeholders to develop a structure that any organization, large or small, in any one of the varied critical infrastructure sectors can use to begin, or make improvements to,

their current cybersecurity programs. The Framework offers a common language to address and manage cyber risks in a cost-effective way based on business needs without placing additional compliance obligations on businesses.

We found that the voluntary nature of the Framework has encouraged the widest set of stakeholders to come to the table and work collaboratively. This approach, with its reliance on voluntary standards, is already consistent with U.S. policy and business use because they have proven to work. Time and time again, when industries get together and determine for themselves what standards describe a quality product, those standards are much more likely to be adopted quickly and to be fully implemented.

I would like to make one other key point. The Framework was designed with the nation's critical infrastructure in mind. But it also can be used by any organization, regardless of its role in society. The broader the effective use of the Framework and its underlying capabilities, the greater the likelihood that our Nation's infrastructure will be secure.

Framework Development Process

Going back to the title of the hearing, I would like to talk about the public-private partnership that the Administration used to develop the Framework. NIST began the process with a Request for Information and received hundreds of submissions from stakeholders in industry, academia, and government. Those submissions, which we posted publicly, provided a foundation for the Framework. But it was only a start; supporting and building on that initial dialogue, we held five workshops around the country with thousands of participants, providing draft versions of the Framework and supporting material multiple times on our website, encouraging comments on all of the material, and carefully considering all the feedback we received.

Organizations across the critical infrastructure, large and small, in many sectors, academia and government were consulted and involved from start to finish. Much of that engagement included international organizations and even other countries. This is a good thing: by having international scale it can be further embraced by the market, creating a suite of truly interoperable products that can be leveraged by anyone.

The Framework

The result of this effort is a document that lays out the critical elements of any cybersecurity program and then links those elements to proven standards and protections for organizations to consider using.

This approach reinforces key processes that all organizations consider as they balance risk to be effective. Through this view, it allows senior leadership's engagement in the cybersecurity risk management process, provides a mechanism to provide accountability and responsibility, and tools for the fusion of threat and vulnerability information with potential impact to business needs and operational capabilities.

The Framework consists of three parts: the Framework Core, the Framework Profiles, and the Framework Tiers.

The Framework Core consists of five Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. While they do not replace a risk management process, these five high-level Functions can also help an organization answer fundamental questions, including "How are we doing?" Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary. The Framework Core also provides additional detail, all the way down to the technical implementation as reflected in standards and guidelines, on how a security program can be created. An example from the "Respond" function is below.

RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5

Figure 1: Example from the Framework Core

Framework Implementation Tiers then provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. During the Tier selection process, an organization will consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. These Tiers reflect a progression from informal, reactive implementations to approaches that are agile and threat-informed.

A Framework Profile represents the outcomes that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Most importantly, profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the desired state). Organizations can use that information to develop action plans to strengthen existing cybersecurity practices and reduce cybersecurity risk. Organizations may also find that they are overinvesting to

achieve certain outcomes and can reprioritize resources to strengthen other cybersecurity practices.

As part of the ongoing work, we believe that organizations will draft sample profiles to illustrate sector-specific needs and requirements – including regulatory and legal obligations.

It is also important to note that the Framework offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity operations. While processes and existing requirements will differ, the Framework can assist organizations in considering privacy and civil liberties as part of a comprehensive cybersecurity program – highlighting risks to privacy and civil liberties that can emerge when developing such a program and helping to mitigate them.

Together we think this structure will enable organizations to improve their practices. By mapping their individual cybersecurity programs against the full list of cybersecurity functions, categories, and specific standards, companies can identify gaps and tailor improvement plans to their specific needs. They can then create internal metrics to track and document those improvements. Some companies may discover in the process that their entire cybersecurity effort consists only of passwords and antivirus software with no real-time detection capability even though automated tools are widely available and affordable. Other companies may find the Framework a useful tool for holding their suppliers accountable or for purchasing these services in a more systematic way.

The bottom line is that we believe the Framework can provide an agreed-upon way to talk clearly to one another about cybersecurity issues and solutions. This in turn, we believe will help us make great strides in strengthening the security and resilience of Critical Infrastructure from cyberthreats.

Next Steps for the Framework

While today's Framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government, it is just another step in a continuous process to improve the Nation's cybersecurity. The Framework is a living document that will need to be updated to keep pace with changes in technology, threats and other factors, and to incorporate lessons learned from its use. These updates will ensure the Framework meets the needs of critical infrastructure owners and operators in a dynamic and challenging environment.

Today, many organizations, led by their senior executives, are using the Framework and providing feedback to NIST and the Department of Homeland Security. This will help us identify improvements needed in the Framework. Industry groups, associations, and non-profits are playing key roles in assisting their members to understand and use the Framework. They are building or mapping their sector's specific standards, guidelines and best practices to the Framework. They are developing and sharing examples of how organizations are using the Framework.

In developing the Framework we also understood that many issues would require additional work with our stakeholders before they could be included in the Framework. These issues became a Roadmap to accompany the Framework that we released on February 12th. This companion Roadmap for the Framework captures NIST's future directions and plans for the Framework and identifies the most important areas for development, alignment, and collaboration. In the near-term, NIST will continue to serve as a convener and coordinator to work with industry and other government agencies to help organizations understand, use and improve the Framework. But we will also hold discussions of models for future governance of the Framework, such as potential transfer to a non-government organization. Like the Framework itself, these plans are based on input and feedback received from the private sector as well as other government agencies. The Roadmap lays out a path toward an improved Framework and a fully developed and functioning ecosystem to support voluntary use of – and improvements to – that document.

The Cybersecurity Framework and its accompanying Roadmap represent a piece of a continuing conversation about how to better protect those critical assets. We look forward to continuing to work collaboratively with industry and government to lower cybersecurity risks and better protect our economy and national security.

Other NIST Public–Private Partnerships in Cybersecurity

NIST's strong partnerships with industry, academia, and government are vital to the success of all our cybersecurity programs in cybersecurity. This reflects our traditional role in innovative research leading to the development of standards and best practices for Federal Departments and Agencies, as well as new programs, notably the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the National Cybersecurity Center of Excellence (NCCoE).

The E-Government Act, Public Law 107-347 recognized the importance of information security to the economic and national security interests of the United States. The Federal Information Security Management Act (FISMA) of 2002, title III of the E-Government Act included duties and responsibilities for the NIST to develop standards and guidelines for Federal information systems.

The NIST Special Publications (SPs) and Interagency Reports provide those management, operational, and technical security guidelines for Federal agencies and cover a broad range of topics such as BIOS management and measurement, cryptography, key management, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, usability, supply chain risk management, authentication, access control, security automation and continuous monitoring.

Beyond these documents, which are peer-reviewed throughout industry, government, and academia, NIST conducts workshops, awareness briefings, and outreach to ensure

comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner.

It is important to note that the impact of NIST's activities under FISMA extend beyond providing the means to protect Federal information technology systems. They provide the cybersecurity foundations for the public trust that is essential to our realizing the national and global productivity and innovation potential of electronic business and its attendant economic benefits. As we further learned in the Framework development process, many organizations voluntarily follow these standards and guidelines, a reflection of their wide acceptance throughout the world.

Beyond the responsibilities under FISMA, under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and related OMB Circular A-119, NIST is tasked with the key role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies such as the State Department to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security and resiliency of this global infrastructure and makes us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation – allowing a market to flourish to create new types of secure products for the benefit of all Americans.

In addition, further development of underlying cybersecurity standards will be needed to improve the security and resiliency of critical U.S. information and communication infrastructure. The availability of cybersecurity standards and associated conformity assessment schemes is essential in these efforts, which NIST supports to help enhance the deployment of sound security solutions and builds trust among those creating and those using the solutions throughout the country.

National Strategy for Trusted Identities in Cyberspace

NIST also houses the National Program Office established to lead implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC is an initiative that aims to address one of the most commonly exploited vectors of attack in cyberspace: the inadequacy of passwords for authentication.

Poor authentication mechanisms are a commonly exploited vector of attack by adversaries. The 2013 Data Breach Investigations Report (conducted by Verizon in concert with the U.S. Department of Homeland Security) noted that in 2012, 76% of network intrusions exploited weak or stolen credentials. In line with the results of this report, Target has revealed that this was the vector taken by its attacker, with a compromised credential of one of its business partners being used to access its network.

NSTIC aims to address this issue by collaborating with the private sector to catalyze a marketplace of better identity and authentication solutions – an "Identity Ecosystem" that raises the level of trust associated with the identities of individuals, organizations, networks, services, and devices online. NIST has funded a dozen pilots and supported work in the privately-led Identity Ecosystem Steering Group (IDESG) to craft standards to improve authentication online.

National Cybersecurity Center of Excellence

In 2012, The National Cybersecurity Center of Excellence (NCCoE) was formed as a partnership between NIST, the State of Maryland, and Montgomery County to accelerate the adoption of security technologies that are based on standards and best practices. The center is a vehicle for NIST to work directly with businesses across various industry sectors on applied solutions to intractable cybersecurity challenges. Today the NCCoE has programs working with the healthcare, financial services, and energy sectors in addition to addressing challenges that cut across sectors including: mobile device security, software asset management, cloud security, and identity management. We are also working to show how these technologies can assist in the implementation of the Cybersecurity Framework.

Conclusion

We at the NIST, and our colleagues within the Department of Commerce, recognize that the cybersecurity challenge facing this Nation is greater than it has ever been. We are committed to listening to the private sector and to working as part of the private-public sector team to address this challenge. In particular, NIST will continue to support a comprehensive set of technical solutions, standards, guidelines, and best practices that are necessary to address this challenge.

Thank you for the opportunity to testify today on NIST's work to develop and advance the use of the *Framework for Improving Critical Infrastructure Cybersecurity* and related activities. I would be happy to answer any questions you may have.

United States Government Accountability Office

GAO

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, March 26, 2014

CRITICAL INFRASTRUCTURE PROTECTION

Observations on Key Factors in DHS's Implementation of Its Partnership Approach

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice

and

Gregory C. Wilshusen, Director
Information Security Issues

GAO Highlights

Highlights of GAO-14-468T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Federal efforts to protect the nation's critical infrastructure from cyber threats have been on GAO's list of high-risk areas since 2003. Critical infrastructure is assets and systems, whether physical or cyber, so vital to the United States that their destruction would have a debilitating impact on, among other things, national security and the economy. Recent cyber attacks highlight such threats. DHS, as the lead federal agency, developed a partnership approach with key industries to help protect critical infrastructure.

This testimony identifies key factors important to DHS implementation of the partnership approach to protect critical infrastructure.

This statement is based on products GAO issued from October 2007 to March 2014. To perform this work, GAO reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs. GAO interviewed DHS officials responsible for administering these programs and assessed related data. GAO also interviewed and surveyed a range of other stakeholders, including federal officials, industry owners and operators, industry groups, and cybersecurity experts.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen its partnership efforts. DHS generally agreed with these recommendations and reported actions or plans to address many of them. GAO will continue to monitor DHS efforts to address these recommendations.

View GAO-14-468T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov, or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

March 26, 2014

CRITICAL INFRASTRUCTURE PROTECTION

Observations on Key Factors in DHS's Implementation of Its Partnership Approach

What GAO Found

GAO's prior work has identified several key factors that are important for the Department of Homeland Security (DHS) to implement its partnership approach with industry to protect critical infrastructure. DHS has made some progress in implementing its partnership approach, but has also experienced challenges coordinating with industry partners that own most of the critical infrastructure.

- **Recognizing and Addressing Barriers to Sharing Information.** Since 2003, GAO has identified information sharing as key to developing effective partnerships. In July 2010, GAO reported some barriers affecting the extent to which cyber-related security information was being shared between federal and industry partners. For example, industry partners reported concerns that sharing sensitive, proprietary information with the federal government could compromise their competitive advantage if shared more widely. Similarly, federal partners were restricted in sharing classified information with industry officials without security clearances. GAO recommended that DHS work with industry to focus its information-sharing efforts. DHS concurred and has taken some steps to address the recommendation, including sponsoring clearances for industry.

- **Sharing Results of DHS Assessments with Industry.** GAO has found that DHS security assessments can provide valuable insights into the strengths and weaknesses of critical assets and drive industry decisions about investments to enhance security. In a May 2012 report, GAO found that DHS was sharing the results of its assessments with industry partners, but these results were often late, which could undermine the relationship DHS was attempting to develop with these partners. GAO recommended that DHS develop time frames and milestones to ensure the timely delivery of the assessments to industry partners. DHS concurred and reported that it has efforts underway to speed the delivery of its assessments.

- **Measuring and Evaluating Performance of DHS Partnerships.** GAO's prior work found that taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In an April 2013 report, GAO examined DHS's chemical security program and assessed, among other things, the extent to which DHS has communicated and worked with industry owners and operators to improve security. GAO reported that DHS had increased its efforts to communicate and work with industry to help them enhance security at their facilities. However, GAO found that DHS was not obtaining systematic feedback on its outreach. GAO recommended that DHS explore opportunities and take action to systematically solicit and document feedback on industry outreach. DHS concurred and reported that it had taken action to address the recommendation.

However, the cyber security of infrastructure remains on GAO's high-risk list and more needs to be done to accelerate the progress made. DHS still needs to fully implement the many recommendations on its partnership approach (and other issues) made by GAO and inspectors general to address cyber challenges.

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to discuss key factors in the Department of Homeland Security's (DHS's) implementation of partnership efforts to protect critical infrastructure from cyber attacks. Critical infrastructure is assets and systems, whether physical or cyber, that are so vital to the United States that their destruction would have a debilitating impact on, among other things, national security or the economy.[1]

Protecting the cybersecurity of our critical infrastructure is a top priority for the nation. For example, in February 2013, the President issued two policies—Executive Order 13636: *Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive PPD21: Critical Infrastructure Security and Resilience* —that aim to increase the overall security and resilience of U.S. critical infrastructure, including cyber security. Moreover, in February 2014, DHS partnered with the critical infrastructure community and established a voluntary program to strengthen critical infrastructure cybersecurity. The DHS Critical Infrastructure Cyber Community Voluntary Program is intended to be the coordination point within the federal government for partnering with critical infrastructure owners and operators interested in improving their cyber risk management processes.

We have recently testified that the federal government must address pressing challenges with cybersecurity and accelerate its progress in bolstering the cybersecurity posture of the nation.[2] As computer technology has advanced, our nation's critical infrastructures such as power distribution, water supply, telecommunications, and emergency services have become increasingly dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is essential to protecting national security, economic prosperity, and public health and safety. We have reported that (1) cyber threats to critical infrastructure are evolving and growing, (2) cyber

[1]See 42 U.S.C. § 5195c(e).

[2]GAO, *Government Efficiency and Effectiveness: Views on the Progress and Plans for Addressing Government-wide Management Challenges*, GAO-14-436T (Washington, D.C.: March 12, 2014).

incidents affecting computer systems and networks continue to rise, and (3) the federal government continues to face challenges in a number of key aspects of its approach to protecting the nation's critical infrastructure.[3]

Since 2003, we have identified protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP—as a government-wide high-risk area, and we continued to do so in the most recent update to our high-risk list.[4] Since that time, the challenges and complexity of developing effective partnerships among the federal government, state and local governments, and industry owners and operators of our nation's critical infrastructure have remained. Our work has shown that trusted relationships are the centerpiece to the ability to share information—in particular information that private entities typically do not want to share and the barriers government faces to sharing. Further, improving information sharing is important, because information on threats and incidents experienced by others can help stakeholders identify trends, better understand the risks they face, and determine what preventive measures should be implemented. DHS's partnership approach is the way in which the federal and state governments and industry stakeholders develop, implement, and maintain a coordinated national effort to manage the risks to critical infrastructure.

My testimony today summarizes prior relevant work and provides our observations on three key factors that are important to DHS's implementation of its partnership approach to protect critical infrastructure from cyber attacks. Specifically, I will address the following factors: (1) recognizing and addressing barriers to sharing information, (2) sharing results of DHS assessments with industry and other stakeholders, and (3) measuring and evaluating the performance of DHS partnerships.

[3]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2103).

[4]GAO's biennial high-risk list identifies government programs that have high vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See, most recently, GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb.14, 2013).

This statement is based on reports we issued from October 2001 to March 2014 related to multiple aspects of DHS efforts to implement its partnership approach to protect critical infrastructure. To perform the work for our previous reports, among other things, we reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs to protect critical infrastructure. We also interviewed DHS officials responsible for administering these programs and obtained and assessed data on the conduct and management of DHS's security-related programs. We also interviewed and surveyed a range of other stakeholders, including federal officials, industry owners and operators, industry group officials, and cybersecurity experts. Further details on the scope and methodology for the previously issued reports are available within each of the published products.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal law and policy have established roles and responsibilities for federal agencies to work with industry in enhancing the physical and cyber-security of critical government and industry infrastructures. For example, consistent with law, presidential policies stress the importance of coordination between the government and industry to protect the nation's cyber critical infrastructure. In addition, policies establish DHS as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation efforts, and recovery efforts for government and industry critical infrastructure and information systems. Federal policy also establishes critical infrastructure sectors, assigns federal agencies responsibilities over each sector (known as sector-specific agencies), and encourages industry involvement.

A fundamental component of DHS's efforts to protect and secure our nation's infrastructure is its partnership approach, whereby it engages in partnerships among government and industry stakeholders. In 2006, DHS

issued the *National Infrastructure Protection Plan* (NIPP),[5] which provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.[6] The NIPP also outlines the roles and responsibilities of DHS with regard to critical infrastructure protection and resilience and sector-specific agencies—federal departments and agencies responsible for critical infrastructure protection and resilience activities in 16 critical infrastructure sectors—such as the dams, energy, and transportation sectors. Appendix I lists the 16 critical infrastructure sectors and their sector-specific agencies. The NIPP emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments. The NIPP also stresses a partnership approach between the federal and state governments, and industry stakeholders for developing, implementing, and maintaining a coordinated national effort to manage the risks to critical infrastructure.

Specific laws and directives have guided DHS's role in critical infrastructure protection, including the Homeland Security Act of 2002, as amended; Homeland Security Presidential Directive/HSPD-7; Presidential Policy Directive/PPD-21, which was issued on February 12, 2013; and Executive Order 13636, which was also issued on February 12, 2013. PPD-21 directs DHS to, among other things, coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. PPD-21 also recognizes that DHS, in carrying out its responsibilities under the Homeland Security Act, evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security

[5]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS issued the NIPP in response to the Homeland Security Act of 2002, as amended, and other authorities and directives. See, e.g., Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146 (2002) (codified at 6 U.S.C. § 121(d)(5)). DHS updated the NIPP in January 2009 to include a greater emphasis on resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). DHS further updated the NIPP, which is now called the National Plan, in December 2013. See DHS, *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[6]According to DHS, in this context, resilience is the ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions. See DHS, Risk Steering Committee, *DHS Risk Lexicon* (Washington, D.C.: September 2010).

and resilience functions that are necessary for effective stakeholder engagement with all critical infrastructure sectors; integrates and coordinates federal cross-sector security and resilience activities; and identifies and analyzes key interdependencies among critical infrastructure sectors, among other things. Executive Order 13636 directs DHS to, among other things, develop a voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness, and quality of cyber threat information sharing; and incorporate privacy and civil liberties protections into every initiative to secure our critical infrastructure.

Within DHS, the National Protection and Programs Directorate (NPPD) is responsible for working with public and industry infrastructure partners and leads the coordinated national effort to mitigate risk to the nation's infrastructure through the development and implementation of the infrastructure protection program. Using a partnership approach, NPPD works with owners and operators of the nation's infrastructure to develop, facilitate, and sustain strategic relationships and information sharing, including the sharing of best practices. NPPD also works with government and industry partners to coordinate efforts to establish and operate various councils intended to protect infrastructure and provide infrastructure functions to strengthen incident response.

Observations on Key Factors in DHS Implementation of Its Partnership Approach

Our prior work has found that DHS and its partners have taken a number of steps intended to improve the security of our critical infrastructure. However, we have also identified a number of additional steps DHS could take to further improve its partnerships aimed at protecting our critical infrastructure. Specifically, our work has identified three key factors that can affect the implementation of the partnership approach used by DHS: (1) recognizing and addressing barriers to sharing information; (2) sharing the results of DHS assessments with industry and other stakeholders; and (3) measuring and evaluating the performance of DHS's partnership efforts.

Recognizing and Addressing Barriers to Sharing Information

Addressing pervasive and sustained computer-based and physical attacks to systems and operations and the critical infrastructures they support depends on effective partnerships between the government and industry owners and operators of critical infrastructure. Recognizing and addressing barriers to information sharing includes, among other things, identifying barriers to sharing information with partners, understanding

information requirements, and determining partners' reasons for participating in voluntary programs.

- **Identifying barriers to industry sharing information with federal partners.** In a July 2010 report examining, among other things, government stakeholders' expectations for cyber-related, public-private partnerships we identified some barriers to industry's sharing of cyber threat information with federal partners.[7] We found that many of the government entities we contacted reported that industry partners were mostly meeting their expectations in several areas, including sharing timely and actionable cyber threat information, though the extent to which this was happening varied by sector. However, we found that federal officials also reported that improvements could be made. For example, while timely and actionable cyber threat and alert information was being received from industry partners, federal officials noted there were limits to the depth and specificity of the information provided by industry partners. Among other issues, we found that industry partners did not want to share their sensitive, proprietary information with the federal government. For example, information security companies had concerns that they could lose a competitive advantage by sharing information with the government if, in turn, this information was shared with those companies' competitors. In addition, despite special protections and sanitization processes, we found that industry partners were unwilling to agree to all of the terms that the federal government or a government agency requires to share certain information. On the basis of our findings, we recommended, among other things, that DHS, in collaboration with industry partners, use the results of our July 2010 report to continue to focus its information-sharing efforts on the most desired services. DHS concurred with this recommendation and described steps underway to address it, including the initiation of several pilot programs intended to enable the mutual sharing of cybersecurity information at various classification levels.

- **Identifying barriers to the government's sharing information with industry partners.** Federal efforts to meet the information-sharing expectations of industry partners are equally important in managing

[7]GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628 (Washington, D.C.: July 15, 2010).

effective public-private partnerships to successfully protect cyber-reliant critical assets from a multitude of threats. In July 2010, we also examined industry partners' expectations for cyber-related, public-private partnerships and identified some barriers to the federal government's sharing of cyber threat information with its industry partners.[8] We reported that federal partners were not consistently meeting industry's information sharing expectations, including providing timely and actionable cyber threat information and alerts, according to industry partners we contacted at the time. We found that this was, in part, due to restrictions on the type of information that can be shared with industry partners. We reported that according to federal officials, DHS's ability to provide information is affected by restrictions that do not allow individualized treatment of one industry partner over another industry partner—making it difficult to formally share specific information with entities that are being directly affected by a cyber threat. In addition, we reported in July 2010 that because DHS has responsibility for serving as the nation's cyber analysis and warning center, it must ensure that its warnings are accurate.[9] Therefore, DHS subjects its products to a stringent review and revision process that can adversely affect the timeliness of its products—potentially adding days to the release if classified, law enforcement, or other information must be removed from the product. In addition, we found that federal officials are restricted to sharing classified information with industry officials in possession of appropriate security clearances and are hesitant to share sensitive information with industry partners, in part, because of the fear that sensitive information shared with corporations could be shared openly on a global basis. We recommended, and DHS concurred, that it should continue to focus information-sharing efforts on the most desired services, including providing security clearances. DHS reported that, among other things, it had instituted a clearance program for critical infrastructure representatives, such as industry partners, to enable their engagement in analysis of the most sensitive cybersecurity threat information.

[8]GAO-10-628.

[9]As part of its implementation of the cyberspace strategy and other requirements to establish cyber analysis and warning capabilities for the nation, DHS established the United States Computer Emergency Readiness Team (US-CERT) to help protect the nation's information infrastructure. US-CERT is the focal point for the government's interaction with federal and private sector entities 24 hours a day, 7 days a week, and is responsible for providing, among other things, cyber-related analysis, warning, information-sharing, major incident response, and national-level recovery efforts.

- **Understanding the information requirements of industry partners.** In our July 2012 report, we also found that federal officials did not have an adequate understanding of the specific private sector information requirements, which could have an adverse affect on federal partners' ability to meet industry partners' expectations. Specifically we found that multiple industry officials stated that federal partners could improve their methods of acquiring the type of information needed by the industry partners.[10] For example, more specific threat information could be focused on the technology being used by a particular entity or specify that a threat intended to target a particular entity, rather than including broad threat information and alerts. In addition, we reported that this more specific information would focus on the specific needs for each sector rather than all of the sectors getting the same information.

- **Determining why some industry partners do not participate in voluntary assessments.** DHS supports the development of the national risk picture by conducting vulnerability assessments and security surveys[11] to identify security gaps and potential vulnerabilities in the nation's most critical infrastructure. In a May 2012 report, we assessed the extent to which DHS had taken action to conduct these surveys and assessments among high-priority infrastructure, shared the results of these surveys and assessments with asset owners or operators, and assessed their effectiveness.[12] We found that various factors influence whether industry owners and operators of assets participate in these voluntary programs, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority assets declined to participate in security surveys or vulnerability assessments. We concluded that collecting data on the reason for declinations could enhance the overall protection and resilience of those high-priority critical infrastructure

[10]GAO-10-628.

[11]DHS vulnerability assessments are conducted during site visits at individual assets and are used to identify security gaps and provide options for consideration to mitigate these identified gaps. DHS security surveys are intended to gather information on an asset's current security posture and overall security awareness. Security surveys and vulnerability assessments are generally asset-specific and are conducted at the request of asset owners and operators.

[12]GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

assets crucial to national security, public health and safety, and the economy. We recommended, and DHS concurred, that it design and implement a mechanism for systematically assessing why owners and operators of high-priority assets decline to participate, and develop a road map, with time frames and milestones, for completing this effort. DHS stated that it had implemented a tracking system in October 2013 to capture data on the reason for declinations by owners and operators.

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

Sharing Results of DHS Assessments with Industry and Other Stakeholders

Another important factor for DHS's implementation of its partnership approach is sharing information on the results of its security assessments and surveys with industry partners and other stakeholders.

- **Timely sharing of assessment results at the asset level.** DHS security surveys and vulnerability assessments can provide valuable insights into the strengths and weaknesses of assets and can help asset owners and operators that participate in these programs make decisions about investments to enhance security and resilience. In our May 2012 report, we found that, among other things, DHS shares the results of security surveys and vulnerability assessments with asset owners or operators.[13] However, we also found that the usefulness of security survey and vulnerability assessment results could be enhanced by the timely delivery of these products to the owners and operators and that the inability to deliver these products in a timely manner could undermine the relationship DHS was attempting to develop with these industry partners. Specifically, we reported that, based on DHS data from fiscal year 2011, DHS was late meeting its (1) 30-day time frame—as required by DHS guidance—for delivering the results of its security surveys 60 percent of the time and (2) 60-day time frame—expected by DHS managers for delivering the results of its vulnerability assessments—in 84 percent of the instances. DHS officials acknowledged the late delivery of survey and assessment results and said they were working to improve processes and

[13]GAO-12-378.

protocols. However, DHS had not established a plan with time frames and milestones for managing this effort consistent with standards for project management. We recommended, and DHS concurred, that it develop time frames and specific milestones for managing its efforts to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners and operators. DHS stated that, among other things, it deployed a web-based information-sharing system for facility-level information in February 2013, which, according to DHS, has since resulted in a significant drop in overdue deliveries.

- **Sharing information with critical infrastructure partners at the sector level.** Critical infrastructures rely on networked computers and systems, thus making them susceptible to cyber-based risks. Managing such risk involves the use of cybersecurity guidance that promotes or requires actions to enhance the confidentiality, integrity, and availability of computer systems. In December 2011, we reported on cybersecurity guidance and its implementation and we found, among other things, that DHS and the other sector-specific agencies have disseminated and promoted cybersecurity guidance among and within sectors.[14] However, we also found that DHS and the other sector-specific agencies had not identified the key cybersecurity guidance applicable to or widely used in each of their critical infrastructure sectors. In addition, we reported that most of the sector-specific critical infrastructure protection plans for the sectors we reviewed did not identify key guidance and standards for cybersecurity because doing so was not specifically suggested by DHS guidance. Therefore, we concluded that given the plethora of guidance available, individual entities within the sectors could be challenged in identifying the guidance that is most applicable and effective in improving their security and that improved knowledge of the available guidance could help both federal and industry partners better coordinate their efforts to protect critical cyber-reliant assets. We recommended that DHS, in collaboration with government and industry partners, determine whether it is appropriate to have cybersecurity guidance listed in sector plans. DHS concurred with our recommendation and stated that it will work with its partners to determine whether it is appropriate to have cybersecurity guidance

[14]GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: Dec. 9, 2011).

drafted for each sector and, in addition, would explore these issues with the cross-sector community.

- **Sharing certain information with critical infrastructure partners at the regional level.** Our work has shown that over the past several years, DHS has recognized the importance of and taken actions to examine critical infrastructure asset vulnerabilities, threats, and potential consequences across regions. In a July 2013 report, we examined DHS's management of its Regional Resiliency Assessment Program (RRAP)—a voluntary program intended to assess regional resilience of critical infrastructure by analyzing a region's ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions—and found that DHS has been working with states to improve the process for conducting RRAP projects, including more clearly defining the scope of these projects.[15] We also reported that DHS shares the project results of each RRAP project report with the primary stakeholders—officials representing the state where the RRAP was conducted—and that each report is generally available to certain staff, such as sector-specific agencies and protective security advisors[16] within DHS. However, we found that DHS did not share individual RRAP reports more widely with others in similar industry lines, including other stakeholders and sector-specific agencies outside of DHS. We also reported that DHS had been working to conceptualize how it can develop a product or products using multiple sources—including RRAP reports—to more widely share resilience lessons learned to its critical infrastructure partners, including federal, state, local, and tribal officials. DHS further reported using various forums, such as regional conferences or during daily protective security advisor contacts, to solicit input from critical infrastructure partners to gauge their resilience information needs. Due to DHS's ongoing efforts, we did not make a related recommendation in the report. However, we noted that through continued outreach and engagement with its critical infrastructure partners, DHS should be better positioned to understand their needs for information about resilience practices, which would in turn help clarify the scope of work

[15]GAO, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*, GAO-13-616 (Washington, D.C.: July 30, 2013).

[16]A protective security advisor is a DHS field representative. Among other things, they conduct RRAP projects.

needed to develop and disseminate a meaningful resilience information–sharing product or products that are useful across sectors and assets.

- **Sharing information with sector-specific agencies and state and local governments.** Federal sector-specific agencies and state and local governments are key partners that can provide specific expertise and perspectives in federal efforts to identify and protect critical infrastructure. In a March 2013 report, we reviewed DHS's management of the National Critical Infrastructure Prioritization Program (NCIPP)—which identifies and prioritizes a list of nationally significant critical infrastructure each year—to include how DHS worked with states and sector-specific agencies to develop the list.[17] We reported that DHS had taken actions to improve its outreach to sector-specific agencies and states in an effort to address challenges associated with providing input on nominations and changes to the NCIPP list. For example, in 2009, we reported that DHS revised its list development process to be more transparent and provided states with additional resources and tools for developing their NCIPP nominations. Furthermore, DHS provided on-site assistance from subject matter experts to assist states with identifying infrastructure, disseminated a lessons-learned document providing examples of successful nominations to help states improve justifications, and was more proactive in engaging sector-specific agencies in ongoing dialog on proposed criteria changes, among other efforts. However, we also found that most state officials we contacted continued to experience challenges with nominating assets to the NCIPP list using the consequence-based criteria developed by DHS. We reported that DHS officials told us that they recognized that some states are facing challenges participating in the NCIPP program and have taken additional steps to address the issue, including working to minimize major changes to the consequence-based NCIPP criteria; enhancing state participation; and working collaboratively with the State, Local, Tribal and Territorial Government Coordinating Council to develop a

[17]GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 (Washington, D.C.: Mar. 25, 2013).

guide to assist states with their efforts to identify and prioritize their critical infrastructure.[18]

Furthermore, in our January 2014 report reviewing the extent to which federal agencies coordinated with state and local governments regarding enhancing cybersecurity within public safety entities, we determined that DHS shared cybersecurity-related information, such as threats and hazards, with state and local governments through various entities.[19] For example, we found that DHS collected, analyzed, and disseminated cyber threat and cybersecurity-related information to state and local governments through its National Cybersecurity and Communications Integration Center and through its relationship with the Multi-State Information Sharing and Analysis Center. In addition, we reported that DHS's State, Local, Tribal, and Territorial Engagement Office's Security Clearance Initiative facilitated the granting of security clearances to state chief information officers and chief information security officers which allowed these personnel to receive classified information about current and recent cyber attacks and threats. For example, we reported that, according to DHS officials, they have issued secret clearances to 48 percent of state chief information officers and 84 percent of state chief information security officers. Moreover, we reported that DHS provides unclassified intelligence information to fusion centers, which then share the information on possible terrorism and other threats and issue alerts to state and local governments. For example, in March

[18]DHS formed the State, Local, Tribal and Territorial Government Coordinating Council in April 2007 to strengthen sector partnership by bringing together experts from a wide range of professional disciplines that relate to critical infrastructure protection from all levels of government. The State, Local, Tribal and Territorial Government Coordinating Council supports geographically diverse partnerships to ensure state, local, tribal, and territorial officials play an integral role in national critical infrastructure protection and resiliency efforts.

[19]GAO, *Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology*, GAO-14-125 (Washington, D.C.: Jan. 28, 2014).

2013, a fusion center issued a situational awareness bulletin specific to public safety entities.[20]

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

Measuring and Evaluating Performance of DHS Partnerships

Measuring and evaluating the performance of DHS partnerships—by among other things, obtaining and assessing feedback, evaluating why certain improvements are made, and measuring the effectiveness of partnerships and assessment—is another important factor in DHS's implementation of its partnership approach.

- **Obtaining and assessing feedback from industry partners.** Taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In April 2013, we examined DHS's Chemical Facility Anti-Terrorism Standards (CFATS) program and assessed, among other things, the extent to which DHS has communicated and worked with owners and operators to improve security.[21] Specifically, we reported that DHS had increased its efforts to communicate and work with industry owners and operators to help them enhance security at their facilities since 2007. We found that as part of their outreach program, DHS consulted with external stakeholders, such as private industry and state and local government officials to discuss issues that affect the program and facility owners and operators. However, despite increasing its efforts to communicate with industry owners and operators, we also found that DHS had an opportunity to obtain systematic feedback on its outreach. We recommended that

[20]A fusion center is a collaboration of two or more federal, state, local, or tribal government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to receive, gather, analyze, and disseminate information intended to detect, prevent, investigate, and respond to criminal or terrorist activity. DHS's Office of Intelligence and Analysis, through its State and Local Program Office, is responsible for coordinating federal support to fusion centers

[21]GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: Apr. 5, 2013).

DHS explore opportunities and take action to systematically solicit and document feedback on facility outreach. DHS concurred with this recommendation and has actions underway to explore such opportunities to make CFATS-related outreach efforts more effective for all stakeholders.

- **Evaluating why facility-level improvements are made or not made.** According to the NIPP, the use of performance measures is a critical step in the risk management process to enable DHS to objectively and quantitatively assess improvement in critical infrastructure protection and resiliency at the sector and national levels. In our May 2012 report on DHS's efforts to conduct surveys and assessments of high-priority infrastructure assets and share the results, we found that, consistent with the NIPP, DHS has taken action to follow up with participants to gather feedback from asset owners and operators that participated in the program regarding the effect these programs have had on asset security.[22] However, we also found that DHS could consider using this follow-up tool to capture key information that could be used to understand why certain improvements were or were not made by asset owners and operators that have received surveys and assessments. For example, the follow-up tool could ask asset representatives what factors—such as cost, vulnerability, or perception of threat—influenced the decision to implement changes, either immediately or over time, if they chose to make improvements. We concluded that obtaining this information would be valuable to understanding the obstacles asset owners or operators face when making security investments. We recommended, and DHS concurred, that it consider the feasibility of expanding the follow-up program to gather and act upon data, as appropriate, on (1) security enhancements that are ongoing and planned that are attributable to DHS security surveys and vulnerability assessments and (2) factors, such as cost and perceptions of threat, that influence asset owner and operator decisions to make, or not make, enhancements based on the results of DHS security surveys and vulnerability assessments. DHS reported that it had modified the follow-up program to capture data on whether ongoing and planned security enhancements are attributable to security surveys and vulnerability assessments. Furthermore, DHS stated that it had also completed additional modifications to the follow-up tools to more

[22]GAO-12-378.

accurately capture all improvements to resilience as well as information on factors influencing owner and operator decisions to make or not make enhancements.

- **Measuring the effectiveness of sector-level partnerships.** Ensuring the effectiveness and reliability of communications networks is essential to national security, the economy, and public health and safety. In an April 2013 report, we found that while DHS has multiple components focused on assessing risk and sharing threat information, DHS and its sector partners do not consistently measure the outcome of efforts to improve cybersecurity at the sector level.[23] For example, we found that DHS and its partners had not developed outcome-based performance measures related to the cyber protection of key parts of the communications infrastructure sector. We concluded that outcome-based metrics related to communications networks and critical components supporting the Internet would provide federal decision makers with additional insight into the effectiveness of partner protection efforts at the sector level. We recommended that DHS collaborate with its partners to develop outcome-oriented measures for the communications sector. DHS concurred with our recommendation and stated that it is working with industry to develop plans for mitigating risks that will determine the path forward in developing outcome-oriented performance measures for cyber protection activities related to the nation's core and access communications networks.

- **Measuring the effectiveness of regional-level assessments.** Similarly, in our July 2013 report examining DHS's management of its RRAP program, we found that DHS had taken action to measure efforts to enhance security and resilience among facilities that participated in these regional-level assessments, but faced challenges measuring the results associated with these projects.[24] Consistent with the NIPP, DHS performs periodic follow-ups among industry partners that participate in these regional assessments with the intent of measuring their efforts to make enhancements arising out of these surveys and assessments. However, we found that DHS did not

[23]GAO, *Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*, GAO-13-275 (Washington, D.C.: Apr. 3, 2013).

[24] GAO-13-616.

measure how industry partners made enhancements at individual assets that participate in a RRAP project contribute to the overall results of the project. DHS officials stated at the time that they faced challenges measuring performance within and across RRAP projects because of the unique characteristics of each, including geographic diversity and differences among assets within projects. However, we concluded that DHS could better position itself to gain insights into projects' effects if it were to develop a mechanism to compare facilities that have participated in a RRAP project with those that have not, thus establishing building blocks for measuring its efforts to conduct RRAP projects. We recommended that DHS develop a mechanism to assess the extent to which individual projects influenced partners to make RRAP-related enhancements. DHS concurred with our recommendation and reported that it had actions underway to review alternatives, including possibly revising its security survey and vulnerability assessment follow-up tool, to address this recommendation.

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

In closing, the federal government has taken a variety of actions that are intended to enhance critical infrastructure cybersecurity. Improving federal capabilities—through partnerships with industry, among other things—is a step in the right direction, and effective implementation can enhance federal information security and the cybersecurity and resilience of our nation's critical infrastructure. However, more needs to be done to accelerate the progress made in bolstering the cybersecurity posture of the nation. The administration and executive branch agencies need to fully implement the hundreds of recommendations made by GAO and agency inspectors general to address cyber challenges. Until then, the nation's most critical federal and private sector infrastructure systems will remain at increased risk of attack from our adversaries.

Chairman Carper, Ranking Member Coburn, and members of the committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For information about this statement please contact Stephen L. Caldwell, at (202) 512-9610 or CaldwellS@gao.gov, or Gregory C. Wilshusen, at (202) 512-6244 or WilshusenG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions to this work included Edward J. George, Jr., Assistant Director; Michael W. Gilmore, Assistant Director; Hugh Paquette, Analyst-in-Charge; Jose Cardenas; Tom Lombardi; and Erin McLaughlin.

Appendix I: Critical Infrastructure Sectors

This appendix provides information on the 16 critical infrastructure (CI) sectors and the federal agencies responsible for sector security. The *National Infrastructure Protection Plan* (NIPP) outlines the roles and responsibilities of the Department of Homeland Security (DHS) and its partners—including other federal agencies. Within the NIPP framework, DHS is responsible for leading and coordinating the overall national effort to enhance protection via 16 critical infrastructure sectors. Consistent with the NIPP, Presidential Decision Directive/PPD-21 assigned responsibility for the critical infrastructure sectors to sector-specific agencies (SSAs).[1] As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of sector partners to protect 10 of the 16 critical infrastructure sectors. Seven other federal agencies have sole or coordinated responsibility for the remaining 6 sectors. Table 1 lists the SSAs and their sectors.

[1] Issued on February 12, 2013, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, purports to refine and clarify critical infrastructure related functions, roles, and responsibilities across the federal government, and enhance overall coordination and collaboration, among other things. Pursuant to Homeland Security Presidential Directive/HSPD-7 and the *National Infrastructure Protection Plan*, DHS had established 18 critical infrastructure sectors. PPD-21 subsequently revoked HSPD-7, and incorporated 2 of the sectors into existing sectors, thereby reducing the number of critical infrastructure sectors from 18 to 16. Plans developed pursuant to HSPD-7, however, remain in effect until specifically revoked or superseded.

Table 1: Critical Infrastructure Sectors and Sector-Specific Agencies (SSA)

Critical infrastructure sector	SSA(s)[a]
Food and agriculture	Department of Agriculture[b] and the Department of Health and Human Services[c]
Defense industrial base[d]	Department of Defense
Energy[e]	Department of Energy
Government facilities	Department of Homeland Security and the General Services Administration
Health care and public health	Department of Health and Human Services
Financial services	Department of the Treasury
Transportation systems	Department of Homeland Security and the Department of Transportation[f]
Water and wastewater systems[g]	Environmental Protection Agency
Commercial facilities Critical manufacturing Emergency services Nuclear reactors, materials, and waste Dams Chemical	Department of Homeland Security Office of Infrastructure Protection[h]
Information technology Communications	Office of Cyber Security and Communications[i]

Source: Presidential Policy Directive/PPD-21

[a]Presidential Policy Directive/PPD-21, released in February 2013, identifies 16 critical infrastructure sectors and designates associated federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA.

[b]The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[c]The Food and Drug Administration is the Department of Health and Human Services component responsible for food other than meat, poultry, and egg products and serves as the co-SSA.

[d]Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commanders of military forces, or military command and control procedures.

[e]The energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[f]Presidential Policy Directive/PPD- 21 establishes the Department of Transportation as co-SSA with the Department of Homeland Security (DHS) for the transportation systems sector. Within DHS, the U.S. Coast Guard and the Transportation Security Administration are the responsible components.

[g]The water sector includes drinking water.

[h]The Office of Infrastructure Protection is the DHS component responsible for the commercial facilities; critical manufacturing; emergency services; nuclear reactors, materials, and waste; dams; and chemical sectors.

[i]The Office of Cyber Security and Communications is the DHS component responsible for the information technology and communications sectors.

Statement before the
US Senate Committee on Homeland Security
and Governmental Affairs

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure"

Testimony of Elayne M. Starkey, CISSP, Chief Security Officer,
Department of Technology and Information, State of Delaware

March 26, 2014

Good morning Senator Carper, Ranking Member Coburn, and members of the Committee. Thank you for inviting me to your hearing today.

As the Chief Security Officer for the State of Delaware, I can report that we are combatting a greater number of cyber-attacks than ever before. State governments not only host volumes of sensitive data about our citizens, we use the Internet to deliver vital services, and ensure our first responders can access the data they need in crisis situations. State government IT systems are a vital component of the nation's critical infrastructure.

Today, with this testimony, I want to provide the Committee information on the value of public-private partnerships. Cyber threats know no borders, and in our interconnected world where all levels of government work with each other, with private sector partners, and with citizens, the only defense is a multi-sector approach. I view these partnerships as a critical component of the Delaware Information Security Program and I am eager to give you specific examples of what is working in my state.

We have been partnering with the US Department of Homeland Security since our program started in 2004. Over the years, our incident response capabilities have improved significantly by participating in DHS's Cyber Storm Exercises. We have advanced our capabilities, thanks to applying funds from the Homeland Security Preparedness Grant Program to create government-wide programs that better secure our cyber infrastructure. We have used this money for annual employee

awareness training, e-mail phishing simulations, technical training, and exercises that test our ability to detect, respond and recover from a simulated large scale cyber-attack. I am grateful to receive approval for this funding. Delaware, however, is an exception. In contrast, most of my peers in other states report limited success in competing with traditional Emergency Responders for just a small share of the grant funds. I urge Congress to carve out a portion of this funding for states to use exclusively on cyber security initiatives.

One of the things I am most proud of is Delaware's effective outreach and collaboration with local governments and other critical infrastructure providers in the state. We were delighted to be selected to participate in the Community Cyber Security Maturity Model, run by the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio. This program has resulted in training at all levels, exercises, seminars, and cyber conferences that are jointly planned and executed by the community. Our next event is a statewide cybersecurity conference on May 6. This is a day-long education workshop which will bring together state and local governments, law enforcement, military, higher education, healthcare, and other critical infrastructure providers. There is so much momentum here that the team has come together as the "Greater Wilmington Cybersecurity Working Group" and is active all year long.

Cyber Awareness, Education, and Training has been the cornerstone of Delaware's program since its inception. Our campaign is active throughout the year with newsletters, training sessions, and lunch 'n learn workshops. In October, as part of

National Cybersecurity Awareness Month, we ratchet up the program by adding many more education and awareness opportunities, employee scavenger hunts, TV and radio advertising, and even wrapping a Delaware Transit bus with an eye-popping cybersecurity message. This literally becomes a moving billboard, carrying the Internet Safety message to 50,000 motorists each day. And every year we offer an upbeat multi-media interactive presentation on Internet Safety to Delaware elementary schools. Thanks to an army of volunteers from my Department, other state agencies, Dover Air Force Base, and Verizon, we have reached over 25,000 fourth graders over the last 7 years. Verizon's support of this program has been unwavering. We could not have done many of these initiatives without the financial support from the Verizon Foundation and the incredible volunteer support from Verizon employees.

Cybersecurity works best when more people have an understanding of the risks and threats. I am especially appreciative of our strong partnership and collaboration with the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Chief Information Officers (NASCIO), and FBI's InfraGard Program.

My final partnership example is with Higher Education. Five years ago, a team of people came together and discovered we all had a similar passion for attracting and nurturing the next generation of cybersecurity professionals. Today that team has evolved into a Coordinating Council that includes all Delaware Universities and Colleges. And together with the Council on Cybersecurity and SANS Institute, we

are planning our 5th annual summer US Cyber Challenge, a week-long, intensive camp filled with specialized security training intended to reduce the shortage in the cyber workforce.

This Saturday a select group of university students, returning veterans and job seekers will compete for the JP Morgan Chase Cyber Aces Governor's Cup. This program is intended to discover and develop talent and provide a pathway to cybersecurity careers.

Governor Markell is hoping to build on all these partnerships. In his January State of the State address, the Governor proposed building a collaborative research and learning network that leverages the public sector, academia, and the private sector. Delaware plans to locate the cyber initiative on the site of a former Chrysler assembly plant that is now owned by the University of Delaware and is already undergoing a transformation from car factory to Research Park. Ultimately, this will help build a skilled cyber workforce that will serve as a pipeline both for the State of Delaware and our businesses, and a hub for cyber innovation.

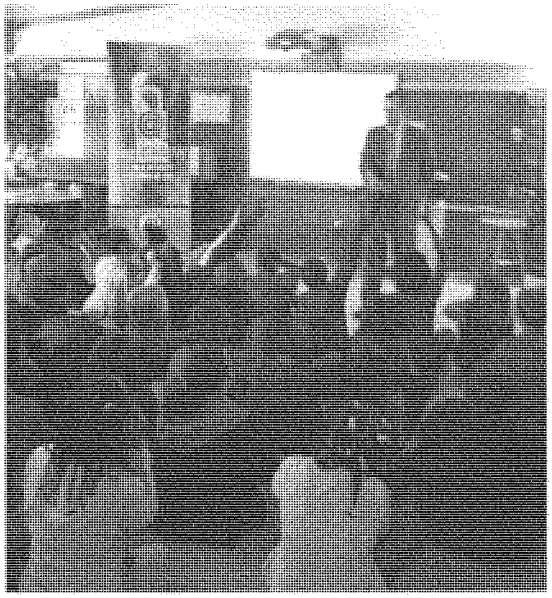
My complements to NIST and DHS and all of the stakeholders that worked together to develop the Cybersecurity Framework. It is valuable to state governments to reference a core set of activities to mitigate against attacks on our systems. For those of us that have established security programs, the Framework will not introduce major changes. Rather, the framework offers valuable risk management

guidance, and is complementary to our Exercise and Incident Response Program. It provides common language, sets a road map, and encourages continuous improvement. It also provides executive-level stakeholders with a succinct explanation of our cyber risk mitigation activities. I endorse the framework as an excellent first step; however, it is important to stress it is a BEGINING and not the END of a process. My hope is that future versions will include incentives to adopt the framework and strive for continuous reduction of cyber risk. I also believe NIST and other key federal agencies can work with states to build tools to assess and demonstrate compliance with standards and best practices. Both the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Association of State Chief Information Officers (NASCIO) are working with federal agencies to achieve these ends.

Cybersecurity is a complex issue, and we have a long road ahead of us to making our nation's systems more secure. It is a journey. It's a race with no finish line. There is no single solution, or a so-called "silver bullet". Holding hearings such as this one and finding ways to share information and resources will be crucial moving forward. I ask that Congress continue to work with the states to identify ways to protect our nation's information assets, and provide funding opportunities for state cybersecurity. Thank you.

Delaware Transit Cybersecurity Buses

4th Grade Internet Safety Presentation



Annual Delaware Cyber Exercise

Testimony of

Steven R. Chabinsky

Before the
United States Senate
Committee on
Homeland Security and Governmental Affairs

"*Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure*"

March 26, 2014

Introduction

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. I am pleased to appear before you today to discuss cybersecurity partnerships among the federal government, states, and the private sector to secure critical infrastructure. In particular, I have been asked to describe my views on partnerships with Federal agencies to increase security and resiliency, including the Cybersecurity Framework and other provisions outlined in the Executive Order issued by President Obama on February 12, 2013.

Background

I have spent over fifteen years committed to reducing the security risks associated with emerging technologies. Most of my efforts have been with the Federal Bureau of Investigation, where I last served as Deputy Assistant Director of the Cyber Division, after having organized and led the FBI's cyber intelligence program and having served as the FBI's top cyber lawyer. Today, I am the General Counsel and Chief Risk Officer of the cybersecurity technology firm CrowdStrike, as well as an adjunct faculty member of George Washington University and the cyber columnist for *Security* magazine. The observations and conclusions I am sharing today in my personal capacity are the culmination of a career spent in government, industry, and academia. It was over 15 years ago that I started to cut my teeth on issues relating to public/private partnerships, then in my capacity as the Principal Legal Advisor to the multi-agency National Infrastructure Protection Center. From that time forward, I have had the privilege of collaborating with the dedicated, patriotic men and woman who have comprised, among other groups, InfraGard, the National White Collar Crime Center (NW3C) and the Internet Crime Complaint Center (IC3), the National Cyber-Forensics & Training Alliance (NCFTA), the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the National Cybersecurity and Communications Integration Center (NCCIC). With that background, what follows are some of my direct observations about the challenges and evolution of our public/private efforts.

The History of U.S. Public-Private Partnerships for Cybersecurity

For quite some time now, government and industry have been investing substantial time and money on public/private cybersecurity partnerships. Indeed, it was back in 1998 that Presidential Decision Directive 63 introduced us to the term "Information Sharing and Analysis Center," or ISAC. Government agencies began to facilitate the creation of sector-specific and multi-sector groups, all with eager anticipation that, by working together, the government and the private sector would prove unstoppable. We believed that through public/private partnerships we could gather, analyze, sanitize and disseminate just the right amount of timely and actionable intelligence to allow the good guys to better defend themselves *while the government identified the bad guys and brought them to justice*.

Noble intentions aside, early in the history of U.S. public/private cyber partnerships, we confronted a host of legal questions that demanded answers. Private sector companies asked whether information sharing partnerships would violate antitrust laws. "No," said the Department of Justice in 2000. Not as long as the information sharing exchanges are open on a non-discriminatory basis to sector members, and are limited to information about security program best practices and the identification of vulnerabilities.

The private sector then expressed concern about the Freedom of Information Act, asking whether the government is required to disclose sensitive information it receives from its industry partners. Again "no," this time from federal courts, which began to hold as early as 1992 that the government can withhold security information from FOIA disclosure as long as the information sharing was voluntary and the company normally would not provide that information to the public. Congress then passed the Critical Infrastructure Information Act of 2002 to statutorily protect certain information from being released under FOIA.

Next came issues of trust, the emergence of legally binding non-disclosure agreements, time-consuming background checks, a review of government classification procedures, consideration of the sticky problem of global companies wanting to share sensitive government threat and vulnerability information with their security officers abroad, as well as our government wanting to share sensitive U.S. business vulnerability information with the law enforcement and intelligence agencies of other countries. Then there were the actual partnership meetings, during which time a significant number of people emerged as free riders who shared nothing and only participated for a chance to mingle and develop business.

As for those participants who truly came to make a difference, the General Accountability Office found that the majority of industry's expectations of working with the government was not being met with respect to the receipt of timely and actionable cyber threat information or cyber alerts. Finally, victim reluctance to report computer intrusions to law enforcement become further exacerbated when the Federal Trade Commission began to eye the corporate victims of cybercrime as "defendants" who

engaged in unfair or deceptive trade practices for lacking effective security, all but eviscerating a decade's worth of confidence building measures by the Department of Justice which had offered constant reassurance that the government's approach is not to blame but to help the victims of cybercrime.

Lessons Learned form Public/Private Partnerships

Fifteen years of lessons-learned have led me to reach a number of conclusions. First, I have found that the most promising joint government/industry outcomes have been and likely will remain at the strategic level rather than at the tactical level. This includes, for example, the sharing and co-development of risk management plans and security best practices, as well as conducting joint incident response training exercises. The Cybersecurity Framework is a shining example of such an effort, prepared by NIST after having worked with over 3,000 individuals and organizations on standards, best practices, and guidelines. I applaud NIST's efforts, and I recommend that every corporate officer and director read the Framework and consider applying its straightforward approach to cybersecurity enterprise risk management.

Second, although we now know that information sharing initiatives between the government and the private sector have inherent limitations when it comes to collecting and disseminating large quantities of time sensitive data for tactical purposes, they are well suited to support collaborative efforts where the parties work together strategically to identify and substantially resolve specific, high-risk, continuing problems. In this regard, a seminal work of public/private collaboration remains the 2009 FBI, FS-ISAC, NACHA joint publication on Automated Clearinghouse Account Hijacking. In that instance, the FBI briefed financial services industry representatives on each of the Bureau's major financial cybercrime cases; the FS-ISAC determined from that what information was timely, unique (meaning not already known by the industry), and relevant for its members; and, together, the FS-ISAC and NACHA recommended solutions that were cost effective and capable of eradicating a problem that otherwise was nearing half a billion dollars in fraud. The key was collaboration, rather than the mere pushing of information. The FBI and industry worked together to identify both the problem and the solution set. Unfortunately today, some five years later, there are indications that it is far more common for government agencies to send information to industry sectors without a coordinated approach as to the information's timeliness, uniqueness, and relevance, and without first obtaining and including industry recommendations on how recipients can best make use of the information and track its utility. As a result, industry is concerned that government information sharing is becoming a numbers game in which the passage of large quantities of "indicators and warning" is viewed in and of itself as a metric of success regardless of outcomes.

Third, while the government often warns the private sector about ongoing or imminent cyber intrusions, more must be done in partnership with the private sector to focus on raising the costs to the attackers. It is time for the government and industry to join

forces to develop and implement technologies and policies that focus less on the vulnerability mitigation aspects relating to information assurance, and more on the threat mitigation aspects of hacker detection, attribution, and punitive response necessary to achieve sustained security. By way of analogy, if foreign fighter planes were on their way to the United States, everyone would be thankful for a government warning to relocate to a bomb shelter. Perhaps sheltering would last for five minutes, or five hours, or even five days, as the government engaged in aerial combat against the threat. But, in cyber, some foreign economic espionage intrusion campaigns have lasted for over ten years, and industry is not seeing from the government an effective plan to confront, repel, and defeat the intruders. To similar effect, Distributed Denial of Service (DDoS) attacks allegedly by North Korea in 2009 and by Iran in 2012 and 2013 have been viewed as the private sector's problem to weather, rather than a confrontation that demanded government engagement.

Fourth, in recognition of the global aspects of both the cyber problem and its solutions, the government and private sector must work together to envision and then drive strategically effective international standards, norms, research and development and multilateral relationships that better position threat deterrent models for the long term. Yet, since 1997, our government has taken concerted actions to privatize and reduce U.S. governance of the Internet. As a result, despite the right aspirational language in the President's 2011 International Strategy for Cyberspace, it is not evident how "the United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits." To date, the inescapable truth is that the risks associated with attacking and exploiting U.S. networks have been negligible, and the private sector has been left largely on its own – under the threat of government regulation and class action lawsuits no less – to defend itself against all enemies.

The Need to Reassess Our Public/Private Cyber Partnerships

1) The Need to Focus on Threat Deterrence Instead of Vulnerability Mitigation

In light of the fact that our increased cybersecurity efforts have not led to a leveling off (no less a reduction) of the threat, it makes sense to question our strategy and to get back to basics. In particular, we would do well to consider how we have successfully reduced security risks in other settings and then try to apply those concepts here.

In order to get security risks under control, whether in the "physical" or cyber worlds, security experts rely upon the levers of vulnerability mitigation, threat reduction and, should the first two fail, consequence management. In the physical world, threat reduction – achieved primarily through threat deterrence – has been our predominant approach, and it has been largely successful. Throughout the physical security spectrum, whether describing the safety of nations, businesses, or individuals, safety is most often achieved because potential aggressors are deterred out of fear they will be brought to justice and actual aggressors ultimately are brought to justice. By way

of contrast, our physical safety is not primarily reliant upon missile defense shields, fortresses, and body armor.

Yet, in the area of cybersecurity, vulnerability mitigation has been our nation's predominant approach, both for securing private sector and government systems. We have retained this focus on vulnerability mitigation despite it being well understood that securing networks is a daunting task even for the most experienced. As stated in Verizon's 2013 Data Breach Investigations Report, "breaches are a multi-faceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity." On the technical side—the web servers, e-mail servers, databases, firewalls, routers, embedded network devices, internal networks, global remote access, custom applications, off-the-shelf applications, backup and storage areas, and all telephone, PBX, and VoIP systems require attention. On the human side, the physical infrastructure must be protected, employee accesses and permissions must be restricted, and connections to business and corporate partners (often operating under different legal regimes) have to be managed. Of course, these are just the basics, and each aspect of cybersecurity must be monitored and updated regularly, as the technologies, users, and adversaries change constantly.

In order to reduce the likelihood of harm, information security professionals deploy a wide range of defensive controls. In the risk management community these are commonly referred to as *technical* controls. Examples of technical controls include password access, endpoint activity monitoring, firewalls, and intrusion detection and prevention systems. Technical controls are particularly well suited to reduce the time necessary to detect unlawful activity and to substantially limit the consequences of a successful breach. Still, although technical controls often are a necessary component of security, they are seldom sufficient. Security professionals also commonly deploy *physical* controls (such as locks on doors) and *administrative* controls (such as acceptable computer use policies and pre-employment background checks). To get a better feel for the difficulties of being a cybersecurity professional, it is worthwhile to consider, at the 30,000 foot level, the following seventeen different categories that NIST recommends network defenders review (keeping in mind that each of these is then broken down further into more discrete, tactical methods):

1. access control;
2. awareness and training;
3. audit and accountability;
4. certification, accreditation, and security assessments;
5. configuration management;
6. contingency planning;
7. identification and authentication;
8. incident response;
9. maintenance;
10. media protection;
11. physical and environmental protection;
12. planning;
13. personnel security;
14. risk assessment;
15. systems and services acquisition;
16. system and communications protection; and
17. system and information integrity.

Continuously reviewing and implementing the technical, physical, and administrative controls within each of these seventeen categories is a never-ending and costly process, which ultimately will not eliminate cyber risk entirely.

Making matters worse, as industry and government agencies continue to spend greater resources on vulnerability mitigation, they finds themselves facing the problem of diminishing economic returns and perhaps even negative economic returns. With respect to diminishing returns, information security professionals typically recognize cost effective benefits when applying baseline cybersecurity efforts. However, as companies direct their resources either against low probability events, or on pursuing all available defenses regardless of the ease with which an adversary can counter them, the amount of protection received for each dollar spent becomes progressively smaller and ultimately is worth less than the expenditure. Imagine for example trying to protect a building by spending two million dollars on a 20-foot brick wall. Meanwhile, an adversary can go to a hardware store and for less than one hundred dollars buy a 30-foot ladder.

Far worse though than the concept of diminishing returns is the concept of negative returns, in which well-intentioned efforts actually make the problem worse. Although it often is difficult to convince good people that they are responsible for escalating a problem, consider our brick wall again. What if the defender spent ten million dollars to build an eighty foot wall? Instead of a buying a ninety foot ladder, the adversary might decide to use an explosive devise to get through the wall, perhaps even killing people in the process. Comparing the brick wall to cybersecurity, there is reason to believe that our strategy often has the unintended consequence of threat actors escalating their capabilities and methods, and proliferating advanced malware that is increasingly destructive.

2) The Need for the Government to Provide for the Common Defense

Compounding the unrealistic push for industry to build impervious systems, our government has grown increasingly reliant upon the owners and operators of our networks to be primarily responsible for defending themselves. By way of example, the public/private partnership efforts set out in Presidential Executive Order 13636 are for the government to share enough cyber threat information with specifically targeted U.S. private sector entities "so that these entities may better protect and defend themselves against cyber threats." In this manner, our government cybersecurity strategy risks morphing into a game of hot potato where, instead of the government fulfilling its traditional role of stopping the threat actor, our agencies now quickly pass information along to the targeted victims and wipe their hands of it. Remarkably, the government appears to expect that corporate America will stop well-resourced, determined, sophisticated actors using a defensive paradigm that is exorbitantly expensive, has proven ineffective over time, and has no precedent of success against persistent threats.

For this reason, we should remain skeptical of government efforts that redirect, rather than supplement, our law enforcement and intelligence resources away from their traditional focus on our adversaries. Despite a sincere effort to declassify and deliver thousands of reports to targeted victims, there is little or no support for the proposition that the private sector can convert this information into a meaningful defense of our critical infrastructure against potential acts of terrorism and foreign aggression. The same holds true with respect to government warnings of cybercrime. As an international group of scientists led by the University of Cambridge succinctly wrote in 2012, "we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail."

3) The Need to Incorporate Threat Deterrence into Alternative Architectures

When thinking of cybersecurity, it is worth considering the Nineteenth Century findings of Charles Darwin. Despite the seeming simplicity of the well-known phrase "survival of the fittest," Darwin did not mean to suggest that survival of the fittest should always be considered in terms of health or strength. Rather, the fittest must be considered in terms of being the right fit for a particular purpose. Survival typically requires adaptability in areas other than health or strength, and adaptability can occur by chance or by design. With due consideration of our economic and national security, as well as the health and welfare of the public, our government should be working with the private sector -- by design -- to adapt our security in a manner that best promotes our survival.

Unfortunately, at best we appear to be leaving decisions about the cybersecurity of our nation's critical infrastructure, and potentially therefore our nation's survival, either to chance, to prevailing market forces, or to the world community. At worst, our declining security actually has occurred by our own design. Consider for a moment that, to date, the design elements of our policies, technologies, and resource allocations have focused on functionality, interoperability, bandwidth, speed and, more recently, anonymity and privacy. Our design elements have not focused on the security of our critical infrastructure. These choices – notably applied to a manmade, controllable environment – are directly responsible for the depth and breadth of our current unfavorable cybersecurity situation. Yet, despite our design choices, network security professionals routinely are being asked to do the impossible in the form of building trusted, impenetrable, dynamic, interoperable networks out of untrusted components, within untrusted environments, using untrusted supply chains, that rely upon untrusted vendors and untrusted users.

We would do well to take Darwin's findings to heart, and begin to use our public/private partnerships in part to explore alternative models in which hardware, software, protocols, and policies are adapted to better suit the wide range of global use scenarios relating to security and privacy. For example, it is hard to imagine that to this day computers that are used for transmitting classified information or for enriching uranium can accept the same USB thumb drive and fall victim to the same

malware as a common computer in a public library. We should establish public/private partnerships to determine whether trusted networks require a combination of distinct design elements, to include enhanced identity management, maximized intrusion detection and attribution capabilities, and prioritized actions to locate and penalize bad actors. Similarly, uniquely defined networks operating internationally, with common Terms of Service, might assist nations (and perhaps even non-governmental organizations) agree on principles for transborder access to data in order to prevent imminent danger to life, limb, or property. Regardless of the solution space, the international and multi-disciplinary aspects of these considerations require substantial government leadership and private sector initiative (similar to the origins of the Internet itself.)

4) The Need for Public/Private Partnerships Relating to Emerging Threats

The 9/11 Commission famously reported its belief that the 2001 terrorist attacks revealed four kinds of U.S. Government failures: "in imagination, policy, capabilities, and management." These words come to mind when considering the lack of public/private partnerships that focus on identifying and countering emerging threats.

Although the government undoubtedly recognizes the need to be predictive and preventative in the area of security there is insufficient collaboration, for example, to counter the vast emerging risks presented by purposeful interference. Many of our nation's essential functions are highly dependent upon wireless communications across the electromagnetic (EM) spectrum. The disruption of GPS location and timing information in and of itself could have cascading effects on the synchronization of computer networks (to include those responsible for financial transactions), vehicle tracking, coordinated movement of people and cargoes, law enforcement offender tracking, surveying, precision agriculture, and a host of other disparate services. Additional disruption capabilities, such as through radio frequency jammers, could create "quiet" zones around wireless networks and end-users, preventing the transmission of vital communications from reaching their intended recipients.

On the government side, the multi-agency Purposeful Interference Response Team (PIRT), managed by the Department of Defense, acts as the federal coordination body for cases of suspected purposeful interference with space systems. Still, the full extent of purposeful interference issues and coordinating opportunities appears to be broader than the PIRT's mandate, funding, and authorities. As stated in 2012 by U.S. Navy Admiral Jonathan Greenert: "Inexpensive jammers, signal detectors, computer processors, and communication systems make it easier today for unfriendly states, terrorists, and criminals to affect our ability to use the EM-cyber environment." The same year, Department of Homeland Security (DHS) official Robert Crane expressed that "we must seek ways for protecting radio frequencies with the goal of rapidly identifying, locating, and mitigating interference sources when they occur and ensuring communications, information and navigation capabilities are secure, resilient, and rapidly restored after an incident." DHS seems particularly well suited

to lead such an effort by coordinating actions across the government and with the private sector to better detect, collect, centralize, analyze, and respond to purposeful interference events. Strengthening public/private partnerships to address these and other emerging threats would further reduce the cyber risks to our critical infrastructure.

Conclusion

There is no doubt that cyber threats present considerable risk to our economic and national security interests, and that these threats continue to grow at an alarming rate. Despite billions of dollars of investment in cybersecurity defensive efforts, and the prospect of spending billions of dollars more, many experts see no hope on the horizon that the overall cyber threat against our country will level off, no less begin to decline. It is my professional opinion that this downward spiral is not inevitable and that we can improve our security considerably. However, it also is my professional opinion that improving our security posture requires that to a certain extent we reconsider, rather than simply redouble, the nature of our efforts.

Fundamentally, we need to ensure that our cybersecurity strategies, technologies, market incentives, and international dialogue focus greater attention on the challenges of more quickly detecting and mitigating harm in high risk environments, while in parallel locating and penalizing bad actors. Doing so would align our cybersecurity efforts with the security strategies we use in the physical world. In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. Instead, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry but, through the use of burglar alarms and video cameras, we shift our focus towards instant detection, attribution, threat response, and recovery. When the alarm monitoring company calls a business owner at 3 a.m., it does not say, "We just received an alarm that your front door was broken into. But, don't worry, we've called the locksmith." Rather, it is only obvious, immediately necessary, and the reason people purchase alarm systems, that they call the police to stop the felon. It is surprising then and suggests a larger problem that, in the world of cyber, when the intrusion detection system goes off the response has been to call the Chief Information Security Officer, and perhaps even the CEO, to explain what went wrong and to prevent it from happening again. It is my hope for the future that the blame for, and the costs of, cybercrime will fall more squarely on the offenders than on the victims, that in doing so we will achieve greater threat deterrence, and that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

Testimony of
Doug Johnson
On behalf of the
Financial Services Sector Coordinating Council
Before the
U.S. Senate Committee on Homeland Security and
Governmental Affairs
March 26, 2014

Chairman Carper, Ranking Member Coburn, my name is Doug Johnson, vice president and senior advisor, risk management policy for the American Bankers Association. In that capacity, I currently lead ABA's enterprise risk, physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership. I am testifying today in my capacity as vice chairman of the Financial Services Sector Coordinating Council (FSSCC), which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues, and as a member of the board of directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC), a private corporation that works with government to provide the financial sector with cyber and physical threat and vulnerability information as part of the nation's homeland security and critical infrastructure protection efforts.

I appreciate the opportunity to be here today representing the FSSCC and FS-ISAC. The American Bankers Association is proud of, and committed to, maintaining its leadership role in helping protect our nation's critical financial infrastructure. The deep involvement of ABA in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial operators and trade associations are heavily involved in both. This collaboration includes financial organizations of all sizes. Our diverse sector is made up of organizations of all sizes and types, and ABA has been a primary driver behind expanding the FS-ISAC's reach from under 100 to over 4,700 members to ensure that vital cyber threat information, and the means to defeat those threats, reaches as many financial organizations as possible.

The financial sector shares the committee's commitment to strengthening public-private partnerships to reduce cyber risks to our nation's critical infrastructure. In my testimony, I will discuss:

- The cyber threats we face, both as an industry and as a nation;
- The role FSSCC and FS-ISAC play in fostering the public-private partnership's ability to address these threats; and
- The work currently underway through the National Institute of Standards and Technology (NIST) to create a cybersecurity framework for our nation to help us mitigate threats.

I. The Cyber Threat is Real and Growing

As you are aware, our nation's financial sector experienced a large number of disruptive cyber-attacks in 2012 and 2013, mostly in the form of distributed denial of service, or DDoS attacks. These attacks were designed to disrupt our sector's customer-facing online banking platforms and cause a periodic loss of availability for those customers. These attacks did not compromise the privacy of customer information or the integrity of bank systems. They were, however, large sustained attacks that challenged the resources of the money centers, as well as the regional, and community banks that were targeted.

Many of our efforts in the financial services sector are to ensure that attacks designed to disrupt users do not set the stage for data compromises or attacks on system integrity. We have seen some instances of blended attacks, where DDoS traffic is used as a diversion from a simultaneous attack on high value customers. We are also aware that a DDoS attack can be an attempt to test various points of entry within a financial institution's system for future, more sophisticated attacks. We are always alert for these possibilities and we expect the nature of attacks to change over time with a continued increase in sophistication and strength.

Our sector is also mindful of attacks that have occurred overseas which, if conducted against U.S. financial institutions, could have significant impact on systems and customers. An attack on Saudi Aramco in August of 2012, where a computer virus called Shamoon wiped the data off approximately 30,000 computers, and in March 2013, attacks against South Korean banks,

purportedly by North Korea, shut down ATM systems for several hours and disabled over 3,000 computers. These are just two examples of the types of attacks necessitating a high level of readiness on the part of our government and industries.

As exhibited by the recent breaches of merchant point-of-sale systems, we are also aware that our vulnerability to such attacks are, in many instances, based on security gaps that may exist on the part of merchants, our business or retail customers, or outsourced service providers. Many financial institutions, particularly those that are community-based, are also highly dependent on core banking system processors and internet banking service providers for cybersecurity protection. While the focus of this hearing is understandably on protecting critical infrastructure, it is also important that we strive to protect the entire financial and payment ecosystem and ensure that our partners in the payments system, our customers, critical service providers and other important business partners have appropriate protections against cybersecurity attacks.

II. The Financial Sector Actively Partners with the Public Sector to Address the Cyber Threat

The nature and frequency of the recent cyber-attacks have focused a great deal of financial institution attention on whether our institutions, regardless of size, are properly prepared for such events, and whether we are committing the appropriate level of resources to detect and defend against them. We also continuously assess and refine our preparedness to detect and respond to future attacks and actively engage our government partners in this process. These efforts build on a long-standing, collaborative imperative for the financial sector to protect institutions and customers from physical and cyber events. A significant protection infrastructure, in partnership with government, exists and is continually being improved.

As I have already indicated, in addition to my role at ABA, I am proud to currently serve as the vice chairman of FSSCC. I also serve on the board of its sister organization, FS-ISAC. ABA has been deeply involved in and supportive of these two organizations since their inception.

Established in 2002, FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by

proactively identifying threats and promoting protection, driving preparedness, and collaborating with the U.S. government. The council has over 60 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms. During the past decade, the partnership has continued to grow, both in terms of the size and commitment of its membership and in the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation.[1]

The FSSCC is considered the policy arm of the financial sector in terms of its engagement with the public sector and other critical sectors of the economy. As such, much of 2013 was dedicated to responding to the administration's executive order, particularly regarding the development of NIST's Preliminary Cybersecurity Framework. As I will discuss later in my testimony, our sector is supportive of the administration's and NIST's efforts and will remain engaged as we migrate toward the framework's implementation phase.[2]

FS-ISAC, considered the operational arm of the financial sector for critical infrastructure protection purposes, was established by the sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive (HSPD) 7 and, most recently PPD 21 called upon the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect the U.S. critical infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts and other critical information throughout the financial sector. FS-ISAC has also recently taken over the role of coordinating crisis response for the sector, formerly a responsibility of FSSCC.

---

[1] A copy of the FSSCC 2012-2013 Annual Report is available here: http://fsscc.org/fsscc/reports/2013/FSSCC-Annual-Report-2012-2013.pdf.
[2] The FSSCC letter of support for the NIST Cybersecurity Framework is available here: http://fsscc.org/fsscc/news/2014/FSSCC-PressRelease-NIST_CSF.pdf.

The overall objective of FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared among members, the sector, and its industry and government partners, which ultimately benefits the nation. FS-ISAC information sharing services and activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources and an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner through the FS-ISAC Security Operations Center (SOC);
- Support for information exchanges with various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee (BRC), and the Payments Risk Council (PRC);
- Development of risk mitigation best practices, threat analysis, toolkits, and the preparation of cybersecurity briefings and white papers; and
- Development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;

Our main government partner in FSSCC and FS-ISAC efforts is the Financial and Banking Information Infrastructure Committee (FBIIC), which is led by the U.S. Department of the Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime is essential to FSSCC's success.

In addition to FBIIC and Treasury, FSSCC and FS-ISAC also work closely with the Department of Homeland Security (DHS), United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and

state and local governments. For example, in partnership with DHS, FS-ISAC two years ago became the third ISAC to participate in the National Cybersecurity and Communications Integration Center's (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, now attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government with numerous examples of success. It is for this reason that the FSSCC supports formalization of the NCCIC through legislation.

As part of this partnership, FS-ISAC set up an email listserv with United States Computer Emergency Readiness Team (U.S. CERT) by which actionable incident, threat and vulnerability information is shared between FS-ISAC members and U.S. CERT in near real-time. This listserv also facilitates the information sharing that is already occurring between FS-ISAC members and the NCCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's response to, and communications with, various sectors following the DDOS attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

FS-ISAC and FSSCC have also worked closely with government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services sector personnel. These clearances have been used to brief the private sector on new information security threats and provided useful information to implement effective risk controls to combat these threats.

The FS-ISAC also works very closely with the other critical infrastructure sectors through direct communication with other ISACs, as through the National Council of ISACs. Information about threats, incidents and best practices is shared daily among the ISACs via ISAC analyst calls and a cross-sector information sharing platform. The ISACs also come together during a crisis to coordinate information and share mitigation efforts, as applicable.

Cross-sector cooperation and coordination for homeland security and critical infrastructure protection also occurs through the Partnership for Critical Infrastructure Security (PCIS) Cross-Sector Council. The PCIS Cross Sector Council, through the membership of the individual sector coordinating councils such as the FSSCC, is the collective body of the private critical sectors identified in HSPD 7. The 20 sectors and sub-sectors have unanimously determined this Council to be their means of obtaining the objectives set forth in the Administration's 2013 revision of the National Infrastructure Protection Plan (NIPP) for consultations and collaborative efforts and unified engagement with the Federal government in fulfilling our joint critical infrastructure protection mission.

To reinforce this commitment, the Council is developing a new charter that ensures clarity on the Council's purpose, role, areas of focus, and governance. The Council is also drafting a Memorandum of Understanding with DHS's National Protection and Programs Directorate that: 1.) defines the purpose of the national-level public-private partnership; 2.) sets strategic priorities; 3.) recommends areas of emphasis for the collaborative effort to attain and advance these priorities; 4.) establishes rules of engagement through agreed best practices; and 5.) ensures effective coordination and consultation. We believe these actions will clarify and confirm the critical sectors' commitment to the council and the manner in which the council will operate and communicate - particularly with regard to its public sector partners.

III. The Financial Sector Supports the NIST Cybersecurity Framework

As mentioned earlier in my testimony, FSSCC and FS-ISAC continue to support the goals of the administration and Congress to limit cybersecurity threats to business, our government, and the American people through a more integrated approach.[3] We applaud the release of Executive Order 13636 and believe implementation of the cybersecurity framework envisioned in the order can be an important tool in improving our nation's overall cybersecurity.

[3] The FSSCC Comment Letter in Response to the NIST Request for Information, "Developing a Framework to Improve Infrastructure Cybersecurity" is available here: http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.

Through FSSCC, our sector is committed to working collaboratively with NIST to further improve the framework and our nation's overall cybersecurity posture. We offer the following recommendations to meet our mutual goals:

- **Encourage the development of sector-specific approaches to the framework.** Recognizing the uniqueness of each sector, the FSSCC will develop a sector profile that will map to the framework. An important component of this sector profile will be a determination of how well the framework maps to existing regulatory requirements. Although the financial sector's stringent regulatory requirements are not specifically itemized in the framework, they nonetheless map well to the framework core functions of identify, protect, detect, respond and recover. Many financial firms already organize their cybersecurity functions in a similar matter, for business as well as regulatory purposes.

- **Facilitate automated information sharing.** Typically the time associated with analyzing a specific cyber threat indicator is substantial. As a result, the "Roadmap" developed by NIST in conjunction with the Framework recognizes that the automated sharing of threat indicator information can provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring.

  FS-ISAC recognized this need over 18 months ago and embarked on the design and development of the financial sector's first Cyber Threat Intelligence Repository to automate threat intelligence sharing. Our goal with this automation solution is to help our sector increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

- **Clarify liability protections for sharing cyber threat data.** The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective measures against malicious cyber activity. While the cyber threat data that are shared by the financial services sector are in machine language and not attributable to an individual, clarity concerning liability protections for the sharing of information are still extremely important and transcend our sector.

- **Foster the growth of existing ISACs and encourage the development of similar models for other sectors currently not deemed critical infrastructure.** Through its current role as the chair of the National Council of ISACs, the FS-ISAC strongly supports cross-sector information sharing initiatives. The FS-ISAC is also working with the retail sector to determine how we can best assist merchant information sharing needs.

- **Leverage existing audit and examination processes and encourage complementary, not redundant audit requirements when implementing the framework.** In my testimony I have noted that the framework fits well with existing financial sector regulatory requirements, but we are still concerned that efforts to implement the framework could create a separate certification process that would be layered over – and possibly complicating -existing cybersecurity examinations and extensive internal and external audits that financial sector firms already undergo. In particular, implementation of the framework should not require additional third party audits in order for a company to be eligible for any incentives where existing audit and regulatory examinations are already in place.

- **Create incentives that are tailored to address specific market gaps.** To the extent that adoption of the framework may be induced through incentives, such incentives should strive to be market-based rather than driven by the public sector. For example, insurance underwriters have, without government inducement, already been asking financial firms how they are planning to incorporate the framework into their cybersecurity protection schemes. Other market incentives include firms requiring their significant supply chain partners to incorporate the framework in some fashion. Only when it is determined that there are specific gaps within the market incentives process should the public sector consider stepping in.[4]

- **Foster Research and Development and Workforce Creation.** The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, in its discussion of next steps, also highlights several research and development issues, such as authentication, as well as

[4] The FSSCC Comment Letter in response to the Department of Commerce's Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices, is available here: http://www.ntia.doc.gov/files/ntia/fssc_response_-_doc_noi.pdf.

cybersecurity workforce development. The FSSCC is fully supportive of enhancing cybersecurity research and development, and believes that a skilled workforce is critical as the cybersecurity threat and technology environment evolves. Through its R&D Committee, the council has also identified identity assurance and authentication as an area requiring specific R&D attention and welcomes the opportunity to work with NIST and other stakeholders on building a framework of authentication standards.

IV. Conclusion

Thank you for holding this important hearing. Financial service companies have made cybersecurity a top priority. We have invested an enormous amount of time, energy and money to put in place the highest level of security among critical sectors and exceed the most stringent regulatory expectations placed upon our sector.

We cannot, however, do this alone. As a nation we must compel appropriate international government bodies to align cyber security laws, law enforcement cooperation and mutual recognition, in addition actively prosecuting and punishing those responsible for committing cyber-crimes. Every nation must recognize that its place in the broader global economy depends on its contribution to the stability of and trust in the critical financial infrastructure that is the circulatory system of national and global economic growth. Enforced norms for global cybersecurity collaboration are an essential foundation of that principle.

We look forward to continuing to work with you toward our mutual goal of protecting our nation's critical assets.

Statement for the Record

David Velazquez
Executive Vice President, Power Delivery
Pepco Holdings, Inc.

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"

Before the Committee on Homeland Security and Governmental Affairs
United States Senate
March 26, 2014

Thank you, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. My name is David Velazquez and I have the privilege of serving as Executive Vice President of Power Delivery for Pepco Holdings, Inc. (PHI), an electric utility delivering power to about 2 million customers in the Mid-Atlantic, including Washington, D.C. It is a pleasure to appear before you today to discuss an issue of fundamental significance to the electric utility sector— public-private partnerships to advance the security of the grid.

We know our adversaries are pursuing capabilities to attack, manipulate, or disable assets across the critical infrastructure sectors through cyber means. Complicating the defense of critical infrastructure is the fact that so many of these potential targets are owned and operated by the private sector. That's why it is imperative that government and industry work closely and leverage each other's expertise for the benefit of utility customers and the general public. The government has intelligence-gathering capability and military forces; the utility sector needs the government to help identify threats and provide technological support to assist in the defense of our systems. Similarly, the utility sector has experience operating an electric utility system; the government must depend on this private sector engineering and operational expertise that keeps the grid running reliably in the face of all hazards.

As the utility powering the nation's capital, PHI has been actively engaged in cybersecurity protection and planning and in the advancement of national cybersecurity regulations and legislation for a number of years. In addition to the sensitivity of our service territory, we are a relatively small utility yet we serve customers in four jurisdictions. The thought that in the absence of federal action, each of these jurisdictions could potentially develop its own cybersecurity framework and protocols is daunting. We believe legislation is necessary and commend the work this Committee and others in the House and Senate have done to try to advance legislation. Recognizing, however, the challenge passing cybersecurity legislation entails, PHI has participated in the development and rollout of the cybersecurity Framework released last month pursuant to the President's Executive Order issued last year.

To this end, PHI was very actively involved in the many public information gathering sessions led by the National Institute of Standards and Technology (NIST). We found this NIST-led process to be extremely collaborative, evolutionary, and respectful of the work that the electric utility sector and our regulators had already done in the cyber space. At the February release of the Framework, PHI pledged to be among the first utilities to work with the Department of Homeland Security and Department of Energy to apply the self-assessment process to our operations. Today, that process is ongoing. We believe the Framework allows us another valuable perspective of the cyber problem and is a tool to help us prioritize our activities and allocate our resources in a rigorous and repeatable manner. The voluntary assessment process the Framework sets forth will give our regulators an important means to effectively communicate cybersecurity efforts within the electric sector and other key critical infrastructure sectors. However, for this process to be truly resonant with our regulators, PHI believes it would benefit from some form of standardized third-party verification.

Though the development of the Framework has significantly advanced electric sector interface with the government on cybersecurity, it is not the first example of this public-private partnership. I'd like to take a few moments to share with you some summary comments on some of these additional tools and partnerships.

Critical Infrastructure Protection Standards (CIP)

CIP standards are both mandatory for all owners and operators of Bulk Power System assets, and enforceable by the Federal Energy Regulatory Commission (FERC) with fines of up to $1

million per day. CIP standards are essential for ensuring basic network hygiene and baseline levels of security for the thousands of entities operating the electric grid. However, they alone cannot account for the very dynamic nature of cyber risks. Instead, the electric power sector has seen the value both of implementing CIP standards *and* of developing close working relationships with federal and state governments. These strategic partnerships help to identify vulnerabilities that could be exploited, implement defenses quickly based on the ever-changing threat environment, and respond in a coordinated way to any successful attacks.

National Cybersecurity & Communications Integration Center (NCCIC)

NCCIC serves as a centralized location where operational elements involved in cybersecurity are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. As a critical infrastructure operator, PHI is in the process of obtaining the clearances needed to maintain a seat on the NCCIC floor and thus participate in NCCIC efforts to provide actionable and comprehensive information in real time to advance a whole-of-nation approach to prevention, response, mitigation, and recovery efforts.

Electricity Subsector Coordinating Council (ESCC)

The ESCC is made up of utility CEOs (including PHI's CEO, Joe Rigby) and trade association leaders representing all segments of the industry, actively partnering with government executives to prepare for, and respond to, national-level disasters or threats to the electric grid. In meetings with senior government leaders over the last year, the ESCC has focused its efforts on three areas of industry-government collaboration:

Incident Response: planning and exercising to coordinate responses to an attack

Information Flow: making sure actionable intelligence and threat indicators are communicated to the right people at the right time

Tools & Technology: deploying the proprietary government technologies that enable machine-to-machine information sharing

The establishment of the ESCC has been invaluable, providing a primary liaison for government entities and other sectors to partner at the senior-executive level with the electric utility industry.

Application of Federally Developed Threat Detection Technologies

Though I am not at liberty to discuss the details of the threat detection programs in which we are partnering with various federal agencies, I can say that PHI has been afforded the opportunity to participate in federal security technology applications that allow for both temporary and permanent real-time, machine-to-machine threat detection. These programs allow us, sometimes at a considerable investment of time and money, to avail ourselves of some of the federal government's far superior capacity to monitor cyber systems for bad actors.

Grid-Ex II

Last November, the North American Electric Reliability Corporation (NERC) conducted a large-scale grid security and incident response exercise in which PHI was one of the many voluntary utility participants. The two-day exercise simulated a coordinated physical and cyber attack damaging the bulk power system and causing widespread outages followed by partial restoration and rotating outages. More than 165 organizations across industry and the government participated. One key learning from the exercise was the need for clearer protocols to coordinate governmental roles in the physical defense of privately held critical infrastructure. For instance, though law enforcement authority traditionally escalates from local to state to national as the scope of an incident becomes clear, in the case of a wide-spread or dispersed physical attack on the grid, all levels of government will need to immediately coordinate their efforts to lessen the potential for cascading impacts.

ICS-CERT

PHI is an active participant in ICS-CERT, a program that provides vulnerability information regarding industry control systems. Other assessment programs under ICS-CERT have helped bring awareness to design principles related to cybersecurity and reliability.

Open Issues

The potential roles for government in cybersecurity can be broken down into four areas:

- Standards and voluntary best practices sharing and assessment
- Information sharing

- Event response protocols
- Coordination of jurisdictional issues

The CIP Standards detailed above and the Framework released last month focus largely on the first of these areas. The CIP Standards set some threshold security mandates for bulk power operators, and the Framework is a voluntary tool to assess the application of existing standards and to determine and share best practices. Though these two programs significantly advance cybersecurity preparedness for grid operators, more can and should be done in the other three areas. For instance, though the federally administered technology programs in which a number of electric utilities participate offer some threat information sharing capacity, in the absence of legislation, much is left undefined with regard to data privacy and the liability associated with bi-directional threat information sharing. Similarly, though the NCCIC and ESCC create forums for event response coordination, they do not resolve all jurisdictional issues. Jurisdictional clarity is particularly important for a cyber-event because, unlike natural disasters, a cyber-event could be a crime, a national security incident, or even an act of war. As such, the primary objectives of different state and federal entities could vary greatly. In fact, governmental objectives might even be in conflict with one agency focused on restoring power and another focused on maintaining evidence needed to catch and prosecute attackers. We must have clear protocols for industry-government event response so that when an attack is identified, we can work quickly to contain the damage, begin restoration but so we can do so without destroying the government's capacity to investigate and prosecute the offense.

Finally, while the value of our investment in cybersecurity and response readiness is hard to measure, some assurance of prompt and reasonable recovery of those investments will be imperative. We know that the potential economic impact of a significant attack on the grid is enormous, and— regardless of how much you invest—you can't absolutely eliminate all threat. This is an issue with which the regulators who approve our rates are grappling. Today, our regulators seem willing to acknowledge the value of our investments in cybersecurity. However, as the threat continues to become more sophisticated, our investments will likely rise rapidly, and some systemized form of prompt cost recovery would facilitate our capacity to grow our expertise to align with this rapidly evolving threat.

In summary, PHI has been very active in and benefitted greatly from the growing array of opportunities to partner with federal, state and local authorities to advance our capacity to address threats to the grid. Public-private partnerships have improved cyber threat detection and cyber and physical event preparation and response coordination. However, more can be done. In particular, issues still needing attention include real-time and actionable threat information sharing, liability protection, event response protocols and systemized cost recovery. We look forward to continuing to work with the Administration, this Committee, and your colleagues in the Senate and House to advance legislation to address these open issues and to continue to improve our capacity to protect the grid from these ever-evolving threats.

The Federal Government's Track Record on Cybersecurity and Critical Infrastructure

A report prepared by

the Minority Staff of the Homeland Security and Governmental Affairs Committee

Sen. Tom Coburn, MD, Ranking Member

February 4, 2014

Introduction

In the past few years, we have seen significant breaches in cybersecurity which could affect critical U.S. infrastructure. Data on the nation's weakest dams, including those which could kill Americans if they failed, were stolen by a malicious intruder. Nuclear plants' confidential cybersecurity plans have been left unprotected. Blueprints for the technology undergirding the New York Stock Exchange were exposed to hackers.

Examples like those underscore for many the importance of increased federal involvement in protecting the nation's privately-owned critical infrastructure. But for one thing: Those failures aren't due to poor practices by the private sector. All of the examples below were real lapses by the federal government.

- **The Nuclear Regulatory Commission** stored sensitive cybersecurity details for nuclear plants on an unprotected shared drive, making them more vulnerable to hackers and cyberthieves.
- **The Securities and Exchange Commission** routinely exposed extremely sensitive data about the computer networks supporting the New York Stock Exchange, including NYSE's cybersecurity measures. The information the SEC exposed reportedly could be extremely useful to a hacker or terrorist who wanted to penetrate the market's defenses and attack its systems.
- Last January, hackers gained access to **U.S. Army Corps of Engineers** computers and downloaded an entire non-public database of information about the nation's 85,000 dams — including sensitive information about each dam's condition, the potential for fatalities if breached, location and nearest city.[1]
- Last February, hackers reportedly broke into the national **Emergency Broadcast System**, operated by the **FCC** as the federal government's tool to address Americans in case of a national emergency. The hackers caused television stations in Michigan, Montana and North Dakota to broadcast zombie attack warnings. "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living," an authoritative voice stated in the hacked broadcast message, while the familiar warning beep sounded. "Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous."[2]
- Last March, hackers exploited a vulnerability on web servers belonging to the **National Institute of Standards and Technology (NIST)**, the federal government's authority for federal and private-sector cybersecurity. The servers, which hosted the federal

[1] Senate HSGAC Minority Staff briefing with U.S. Army Corps of Engineers officials, May 3, 2013.
[2] "Local Station Breaks Into Programming With Emergency Zombie Apocalypse Alert," Mediaite.com, February 11, 2013, http://www.mediaite.com/tv/local-montana-station-breaks-into-programming-with-emergency-zombie-apocalypse-alert/, accessed January 13, 2014.

government's database of known software vulnerabilities, had to be taken out of service for several days.[3]

In addition, hackers have penetrated, taken control of, caused damage to and/or stolen sensitive personal and official information from computer systems at the Departments of Homeland Security, Justice, Defense, State, Labor, Energy, and Commerce; NASA; the Environmental Protection Agency; the Office of Personnel Management; the Federal Reserve; the Commodity Futures Trading Commission; the Food and Drug Administration; the U.S. Copyright Office; and the National Weather Service, according to public reporting.[4]

These are just hacks whose details became known to the public, often because the hackers themselves announced their exploits. Largely invisible to the public and policymakers are over 48,000 other cyber "incidents" involving government systems which agencies detected and reported to DHS in FY 2012.[5] And one cannot ignore the universe of other intrusions that agencies could not detect: civilian agencies don't deteet roughly 4 in 10 intrusions, according to testing reported in 2013 by the White House Office of Management and Budget.[6]

While cyber intrusions into protected systems are typically the result of sophisticated hacking, they often exploit mundane weaknesses, particularly out-of-date software. Even though they sound boring, failing to install software patches or update programs to their latest version create entry points for spies, hackers and other malicious actors. Last July, hackers used just that kind of known, fixable weakness to steal private information on over 100,000 people from the Department of Energy. The department's Inspector General blamed the theft in part on a piece of software which had not been updated in over two years, even though the department had purchased the upgrade.[7]

---

[3] Goodin, Dan, "National Vulnerability Database taken down by vulnerability-exploiting hack," Ars Technica, March 14, 2013, http://arstechnica.com/security/2013/03/national-vulnerability-database-taken-down-by-vulnerability-exploiting-hack/, accessed January 13, 2014.

[4] Reported incidents compiled by the Senate Committee on Commerce, 2013; Rosenzweig, Paul, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues," Heritage Foundation, http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue, accessed January 13, 2014; Ryan, Jason, "Anonymous Hits Federal Reserve in Hack Attack," ABCNews.com, Feb. 6, 2013, http://abcnews.go.com/blogs/politics/2013/02/anonymous-hits-federal-reserve-in-hack-attack/, accessed January 13, 2014; Lennon, Mike, "NASA Inspector General Said Hackers Had Full Functional Control Over NASA Networks," SecurityWeek, March 3, 2012, http://www.securityweek.com/nasa-inspector-general-said-hackers-had-full-functional-control-over-nasa-networks, January 13, 2014; Lowenson, Josh, "Lawmakers ask for deeper look into FDA security hack," TheVerge.com, Dec. 9, 2013, http://www.theverge.com/us-world/2013/12/9/5194260/lawmakers-ask-for-deeper-look-into-fda-security-hack, accessed January 13, 2014.

[5] "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, p. 17, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

[6] "Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, p. 30: Across 22 agencies, "on average the NOC/SOC [Network Operations Center/Security Operations Center] was 63% effective at detecting incidents." http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

[7] Goodin, Dan, "How hackers made minced meat out of the Department of Energy networks," Ars Technica, Dec. 16, 2013, http://arstechnica.com/security/2013/12/how-hackers-made-minced-meat-of-department-of-energy-networks/, accessed January 13, 2014.

The President's Order

In February 2012, President Obama unveiled an executive order to protect the nation from debilitating cyberattacks.[8] The president's order addresses the security of computers and networks which run the nation's commercially-owned critical infrastructure. Already, agencies are drawing up plans and working with the private sector to implement the president's directive.

It is appropriate for the White House to envision a federal role in protecting privately-owned infrastructure, particularly when that infrastructure undergirds the nation's economy and society. However, for the country's citizens and businesses to take the government's effort seriously, the federal government should address the immediate danger posed by the insecurity of its own critical networks.

Over more than a decade, the federal government has struggled to implement a mandate to protect its own IT systems from malicious attacks. As we move forward on this national strategy to boost the cybersecurity of our nation's critical infrastructure, we cannot overlook the critical roles played by many government operations, and the dangerous vulnerabilities which persist in their information systems.

Federal Information Security Management Act (FISMA)

Eleven years ago, Congress passed and the White House approved legislation to strengthen the federal government's own computers and networks.[9] The law, known as the Federal Information Security Management Act (FISMA), requires agencies to develop, document, and implement information security programs which meet certain specifications.[10] As Congress again contemplates a major cybersecurity effort, it may be advisable to evaluate how the federal effort has fared. For one thing, FISMA could benefit from reforms of its own. But more importantly, its history can hold clues to the federal government's ability to effectively mandate and enforce cybersecurity standards.

Since 2006, the federal government has spent at least $65 billion on securing its computers and networks, according to an estimate by the Congressional Research Service.[11] The National Institute of Standards and Technology (NIST), the government's official body for setting cybersecurity standards, has produced thousands of pages of precise guidance on every significant aspect of IT security. And yet agencies — even agencies with responsibilities for critical infrastructure, or vast repositories of sensitive data — continue to leave themselves vulnerable, often by failing to take the most basic steps towards securing their systems and information.

Methodology

---

[8] "Executive Order – Improving Critical Infrastructure Cybersecurity," White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, accessed January 13, 2014.

[9] "Federal Information Security Management Act of 2002," enacted as Title III of the E-Government Act of 2002 (Pub.L. 107-347).

[10] "FISMA: Detailed Overview," NIST, http://csrc.nist.gov/groups/SMA/fisma/overview.html, accessed January 13, 2014.

[11] Congressional Research Service, Memo to HSGAC Minority Staff, "FISMA Spending, Historical Trends," June 6, 2013.

This report draws on more than 40 audits and other reviews by agency inspectors general, including mandated annual FISMA audits for nearly a dozen agencies, as well as open-source reporting on cybersecurity and federal agencies. In addition, staff interviewed officials from offices of inspectors general (OIGs) about their cybersecurity work.

Due to the sensitivity of the topic, drafts of this report were shared with relevant OIGs to confirm no sensitive non-public information was inadvertently included which could harm federal cybersecurity efforts.

Department of Homeland Security

In 2010, the Administration tasked the Department of Homeland Security to lead the federal government's efforts to secure its own computers.

Since it was selected to shoulder the profound responsibility of overseeing the security of all unclassified federal networks, one might expect DHS's cyber protections to be a model for other agencies, or that the department had demonstrated an outstanding competence in the field. But a closer look at DHS's efforts to secure its own systems reveals that the department suffers from many of the same shortcomings found at other government agencies.

In August 2010 — just one month after a White House directive gave DHS responsibility for the cybersecurity of all federal government networks — the DHS Inspector General found that the DHS computer security experts who would fulfill that directive had serious cyber vulnerabilities in their own systems. The IG found hundreds of vulnerabilities on the DHS cyber team's systems, including failures to update basic software like Microsoft applications, Adobe Acrobat and Java,[12] the sort of basic security measure just about any American with a computer has performed.

Weaknesses at DHS are not confined to its own cybersecurity office. IT security vulnerabilities exist throughout DHS and its component agencies. Although it has steadily improved its overall cybersecurity performance, DHS is by no means a standard-setter. In fact, in some key areas DHS lags behind many of its agency peers. For instance, in 2013 OMB found DHS rated below the government-wide average for using anti-virus software or other automated detection programs encrypting email, and security awareness training for network users.[13]

In 2013, OMB set a goal for government agencies to send at least 88% of all internet traffic through special secure gateways, known as Trusted Internet Connections (TICs). It set a goal for DHS of 95 percent. The Department's Inspector General reported last November DHS failed to meet either goal. Just 72 percent of DHS internet traffic passed through TICs, the IG stated. It should be noted tbat DHS is responsible for the administration's efforts to consolidate federal internet traffic through TICs.[14]

---

[12] "DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems," DHS Office of Inspector General, August 2010, http://www.oig.dhs.gov/assets/Mgmt/OIG_10-111_Aug10.pdf, accessed January 13, 2014.

[13] "Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002," Office of Management and Budget, March 2013, pp. 31-35, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf, accessed January 13, 2014.

[14] "OIG-14-09: Evaluation of DHS' Information Security Program for Fiscal Year 2013," DHS Office of Inspector General, November 2013, pp. 3, 15, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-09_Nov13.pdf, accessed January 13, 2014. DHS has claimed its TIC consolidation numbers have improved since then.

Repeated failure to install software updates and security patches. In 2012, the IG found vulnerabilities arising from missing patches on computers at the National Protection and Programs Directorate (NPPD), which houses the bulk of DHS's cybersecurity efforts; on servers supporting U.S. Secret Service intelligence work; on computers supporting ICE Homeland Security Investigations' Intelligence Fusion Systems, a powerful system allowing agents to query several sensitive databases; and on dozens of servers supporting TSA's Transportation Worker Identification Credential (TWIC) program, which keeps biometric information and credentials for over two million longshoremen, truckers, port employees, mariners and others.[15]

Sensitive databases protected by weak or default passwords.[16] At NPPD, which oversees DHS's cybersecurity programs, the IG found multiple accounts protected by weak passwords. For FEMA's Enterprise Data Warehouse, which handles reports on FEMA's disaster deployment readiness and generates other reports accessing Personally Identifying Information (PII),[17] the IG found accounts protected by "default" passwords, and improperly configured password controls.[18]

Computers controlling physical access to DHS facilities whose antivirus software was out of date. Twelve of the 14 computer servers the IG checked in 2012 had anti-virus definitions most recently updated in August 2011. Several of the servers also lacked patches to critical software components.[19]

Websites with known types of vulnerabilities which could allow a hacker to hijack user accounts, execute malicious scripts, or access sensitive information.[20] Public websites for CBP, FEMA, ICE and even NPPD, home of US-CERT held flaws which could allow unauthorized access, the IG found in 2012. Notably, several vulnerabilities were found in the DHS website "Build Security In" (http://www.buildsecurityin.us-cert.gov).[21] DHS developed the site to encourage software developers "to build security into software in every phase of its development."[22]

Poor physical and information security. Independent auditors physically inspected offices and found passwords written down on desks, sensitive information left exposed, unlocked

---

[15] ITDashboard, "TSA – Transportation Worker Identification Credential (TWIC)," http://www.itdashboard.gov/investment?buscid=170; TWIC Deployment Website, http://www.twicinformation.com/twicinfo/, accessed January 13, 2014; information provided by DHS Office of Inspector General.

[16] Examples of easily-guessed passwords are a person's username or real name, the word "password," the organization's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology. NIST, "Guide to Enterprise Password Management (Draft), Special Publication 800-118," April 2009, http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-118, accessed January 13, 2014.

[17] "Privacy Impact Assessment for the Operational Data Store (ODS) and Enterprise Data Warehouse (EDW)," June 29, 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_ods_edw_20120629.pdf, accessed January 13, 2014.

[18] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[19] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[20] "Evaluation of DHS' Information Security Program for Fiscal Year 2012," DHS Office of Inspector General, October 2012, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-04_Oct12.pdf, accessed January 13, 2014.

[21] Information provided to HSGAC by DHS Office of Inspector General, February 14, 2013.

[22] "Build Security In," https://buildsecurityin.us-cert.gov/bsi/home.html, accessed January 13, 2014.

laptops, even credit card information. To take just one example, weaknesses found in the office of the Chief Information Officer for ICE included 10 passwords written down, 15 FOUO (For Official Use Only) documents left out, three keys, six unlocked laptops — even two credit cards left out.[23]

[23] "Information Technology Management Letter for the Immigration and Customs Enforcement Component of the FY 2012 Department of Homeland Security Financial Statement Audit," DHS Office of Inspector General, April 2013, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-60_Apr13.pdf, accessed January 13, 2014.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) maintains volumes sensitive, detailed documentation on nuclear facilities. The design and security plans of every nuclear reactor, waste storage facility, and uranium processing facility in the United States; records on every individual licensed to operate or supervise nuclear reactors; and information on the design and process of nuclear material transport all live on the NRC's systems.

Unauthorized disclosure of such sensitive, non-public information "could result in damage to the Nation's critical infrastructure," including nuclear power plants, according to the NRC's Inspector General.[24] Unfortunately, the NRC regularly experiences unauthorized disclosures of sensitive information, or fails to apply adequate measures to protect that data.

Perceived ineptitude of NRC technology experts. There is such "a general lack of confidence" in the NRC's information technology division that NRC offices have effectively gone rogue – by buying and deploying their own computers and networks without the knowledge or involvement of the department's so-called IT experts. Such "shadow IT" systems "can introduce security risks when unsupported hardware and software are not subject to the same security measures that are applied to supported technologies," the NRC Inspector General reported in December 2013. [25]

Sensitive data stored on unsecured shared drive. NRC workers improperly stored and shared sensitive information on an unsecured network drive, according to a 2011 audit. Among the inappropriate data found on the drive: details on nuclear facilities' cybersecurity programs; information on security at fuel cycle facilities; and a Commissioner's passport photo, credit card image, home address and phone number.[26]

Failure to report security breaches. How often does the NRC lose track of or accidentally expose sensitive information to possible release? The NRC can't say, because it has no official process for reporting such breaches. Many involve electronic data stored on the Commission's computers. Of the 95 security lapses which NRC personnel did report between 2005 and 2011, at least a third appear to involve NRC's IT systems.[27]

Inability to keep track of computers. The NRC has had trouble keeping track of its laptop computers, including those which access sensitive information about the nuclear sites the

[24] "Semiannual Report to Congress," Nuclear Regulatory Commission Office of the Inspector General, September 30, 2012, http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1415/v25n2/sr1415v25n2.pdf, accessed January 13, 2014.

[25] "Audit of NRC's Information Technology Governance," Nuclear Regulatory Commission Office of the Inspector General, December 9, 2013, pp. i, 8, http://pbadupws.nrc.gov/docs/ML1334/ML13343A244.pdf, accessed January 13, 2014.

[26] "Audit of NRC's Shared "S" Drive," Nuclear Regulatory Commission Office of the Inspector General, July 27, 2011, http://pbadupws.nrc.gov/docs/ML1120/ML112081653.pdf, accessed January 13, 2014.

[27] "Audit of NRC's Protection of Safeguards Information," Nuclear Regulatory Commission Office of the Inspector General, April 16, 2012, http://pbadupws.nrc.gov/docs/ML1210/ML12107A048.pdf, accessed January 13, 2014.

commission regulates.[28] Confusion over laptops' documentation and authorization "could lead to unauthorized use of NRC resources or release of sensitive information," the NRC OIG warned in 2012.[29]

General Sloppiness. Federal guidelines are clear: when an agency identifies a weakness in its IT security, officials must record the problem, find a way to fix it, and assign themselves a deadline for completion. As officials make progress and the weakness is eventually remedied, officials are supposed to update their records. Without that basic system in place, neither the agency nor the administration can tell if vulnerabilities are being addressed.

Yet just about every aspect of that process appears to be broken at the NRC. Problems were identified but never scheduled to be fixed; fixes were scheduled but not completed; fixes were recorded as complete when they were not. In 2012, the IG reported the NRC was "not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls."[30] Last November, a year later, the IG found that nothing had changed, and that the NRC's efforts "are still not effective at monitoring the progress of corrective efforts … and therefore do not provide an accurate measure of security program effectiveness."[31]

[28] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2012," Nuclear Regulatory Commission Office of the Inspector General, November 8, 2012, pp. 5-6, http://pbadupws.nrc.gov/docs/ML1231/ML12313A195.pdf, accessed January 13, 2014.

[29] "Information of Security Risk Evaluation of Region II – Atlanta, GA," Nuclear Regulatory Commission Office of the Inspector General, August 27, 2012, p. 10, http://www.nrc.gov/reading-rm/doc-collections/insp-gen/2012/oig-12-a-17.pdf, accessed January 13, 2014.

[30] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2012," Nuclear Regulatory Commission Office of the Inspector General, November 8, 2012, http://pbadupws.nrc.gov/docs/ML1231/ML12313A195.pdf, accessed January 13, 2014.

[31] "Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013," Nuclear Regulatory Commission Office of Inspector General, November 22, 2013, http://pbadupws.nrc.gov/docs/ML1332/ML13326A090.pdf, accessed January 13, 2014.

Internal Revenue Service

The Internal Revenue Service (IRS) collects federal taxes owed by any person or business in the United States, and its computers hold more sensitive data on more Americans than those of perhaps any other federal component. In addition to traditional records on employment, income and identifier information, the IRS reportedly collects a huge volume of personal information on Americans' credit card transactions, eBay activities, Facebook posts and other online behavior.[32]

Unfortunately, the IRS has struggled with the same serious cybersecurity issues for years, and has moved too slowly to correct them.

The IRS' internal watchdog, the Treasury Inspector General for Tax Administration (TIGTA), believes data security is the most serious management challenge facing the IRS.[33] For years, the Government Accountability Office (GAO) has also warned IRS its computers are not safe — that in fact, they are dangerously vulnerable to intrusion and data theft.[34]

Every year since 2008, GAO has identified about 100 cybersecurity weaknesses at the IRS which compromise the agency's computers and data, often repeating weaknesses it cited the previous year.[35] Every year, the IRS claims to fix about half of them, but GAO says even those disappointing numbers aren't right, because IRS doesn't confirm the actions they take actually fix the problems.[36] And every year, GAO returns and finds around 100 problems with IRS' cybersecurity.[37]

Fails to enerypt sensitive data. IRS routinely fails to encrypt its data — converting sensitive data into complex code, making it difficult to read without a key to de-encrypt the

---

[32] Satran, Richard, "IRS High-Tech Tools Track Your Digital Footprints," U.S. News and World Report, April 4, 2013, http://money.usnews.com/money/personal-finance/mutual-funds/articles/2013/04/04/irs-high-tech-tools-track-your-digital-footprints, accessed January 13, 2014.

[33] "Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2014," Treasury Inspector General for Tax Administration, November 8, 2013, http://www.treasury.gov/tigta/management/management_fy2014.pdf, accessed January 13, 2014.

[34] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, March 2013, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, http://gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, http://gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

[35] Ibid.

[36] Ibid.

[37] Ibid.

information — or it encrypts the data so weakly that it can be easily decoded.[38] Since at least 2009, GAO has repeatedly identified instances where IRS did not properly encrypt sensitive data including tax, accounting, and financial information, as well as usernames and passwords. Failing to encrypt or weakly encrypting those data makes it easier for a malicious actor to download, view, and possibly even change taxpayer information and IRS systems.[39]

Lousy user passwords. In March 2013, GAO reported that IRS allowed its employees to use passwords that "could be easily guessed." Examples of easily-guessed passwords are a person's username or real name, the word "password," the agency's name, or simple keyboard patterns (e.g., "qwerty"), according to the National Institute of Standards and Technology.[40] In some cases, IRS users had not changed their passwords in nearly two years.[41] As a result someone might gain unauthorized access to taxpayers' personal information and it "would be virtually undetectable," potentially for years.[42] GAO has cited IRS for allowing old, weak passwords in every one of its reports on IRS' information security for the past six years.[43]

Officials don't properly fix known vulnerabilities. IRS employees monitored its computers by running programs which flagged vulnerabilities in equipment and software, but

---

[38] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, March 2013, p. 10, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, p. 9, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, p. 9, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, p. 9, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, p. 11, http://www.gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, p. 12, http://www.gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

[39] Ibid.

[40] NIST, "Guide to Enterprise Password Management (Draft), Special Publication 800-118," April 2009, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf, accessed January 13, 2014.

[41] "INFORMATION SECURITY: IRS Has Improved Controls but Needs to Resolve Weaknesses," Government Accountability Office, pp. 7–8, March 2013, http://www.gao.gov/assets/660/653086.pdf, accessed January 13, 2014.

[42] Ibid.

[43] Ibid; "INFORMATION SECURITY: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2012, p. 7, http://www.gao.gov/assets/590/589399.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data," Government Accountability Office, March 2011, p. 7, http://www.gao.gov/assets/320/316569.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses," Government Accountability Office, March 2010, p. 7, http://gao.gov/assets/310/302087.pdf, accessed January 13, 2014; "INFORMATION SECURITY: Continued Efforts Needed to Address Significant Weaknesses at IRS," Government Accountability Office, January 2009, p. 10, http://www.gao.gov/assets/290/284722.pdf, accessed January 13, 2014; "INFORMATION SECURITY: IRS Needs to Address Pervasive Weaknesses," Government Accountability Office, January 2008, p. 10, http://www.gao.gov/assets/280/270917.pdf, accessed January 13, 2014.

then failed to fix the issues. As a result, scans repeatedly flagged the same vulnerabilities "for two or three consecutive months."[44]

Dangerously slow to install crucial software updates and patches. In March 2012, IRS computers had 7,329 "potential vulnerabilities" because critical software patches had not been installed on computer servers which needed them.[45] At one point in 2011, over a third of all computers at the IRS had software with critical vulnerabilities that were not patched.[46] IRS officials said they expect critical patches to be installed within 72 hours. But TIGTA found it took the IRS 55 days, on average, to get around to installing critical patches.[47] Most recently, in September 2013, TIGTA re-affirmed that the IRS still "has not yet fully implemented a process to ensure timely and secure installation of software patches."[48]

[44] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, pp. 7-8, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[45] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[46] "Federal Information Security Management Act Report for Fiscal Year 2012," Treasury Inspector General for Tax Administration, September 28, 2012, p. 7, http://www.treasury.gov/tigta/auditreports/2012reports/201220114fr.pdf, accessed January 13, 2014.

[47] "An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers," Treasury Inspector General for Tax Administration, September 25, 2012, p. 10, http://www.treasury.gov/tigta/auditreports/2012reports/201220112fr.pdf, accessed January 13, 2014.

[48] "Federal Information Security Management Act Report for Fiscal Year 2013," Treasury Inspector General for Tax Administration, September 27, 2013, p. 7, http://www.treasury.gov/tigta/auditreports/2013reports/201320126fr.pdf, accessed January 13, 2014.

Department of Education

The Department of Education holds and manages $948 billion in student loans made to more than 30 million borrowers. The Department's computers hold volumes of information on those borrowers — loan applications, credit checks, repayment records and more.[49]

Given the mammoth store of sensitive information the department keeps, it is disappointing that its Inspector General has said there is little assurance that sensitive data has not been altered or stolen from the computer systems which undergird its lending program.[50]

"[T]he Department's information is vulnerable to attacks that could lead to a loss of confidentiality," the IG concluded. "Also, there is increased risk that unauthorized activities … could reduce the reliability and integrity of Department systems and data."[51]

No review for malicious activity. The Education Department provides remote access to student financial data to Department officials who are off-site or teleworking. Those remote access accounts can be easily compromised by hackers, who use keylogger malware to steal login information from official's computers by secretly recording their keystrokes.

In 2011 and 2012, The Education Department's Federal Student Aid (FSA) office reported 819 compromised accounts. In only 17 percent of those cases did the Department review activity for those accounts to see whether any malicious activity had occurred.[52] Although the financial data is maintained by outside contractors, some of the Department's contracts for those services don't ensure it has access to audit logs for this purpose.[53]

In fact, the Education Department failed to ensure the contractor properly protected borrowers' sensitive personal and financial information; adequately configured their systems

[49] U.S. Department of Education, Office of Federal Student Aid, *Annual Report 2012*, p. 2, http://www2.ed.gov/about/reports/annual/2012report/fsa-report.pdf, accessed January 13, 2014.

[50] Inspector General Tighe testimony before the House Oversight and Government Reform Committee, March 5, 2013, pages 10-11, http://cq.com/doc/testimony-4230838#testimony, accessed January 13, 2014.

[51] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 9, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[52] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 10, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[53] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 11, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

with security measures; identified and corrected flaws in their IT system; or adequately managed configuration settings and patching updates.[54]

Unsecure networks. Stealing login data wasn't the only way for hackers to potentially compromise the Department's network infrastructure. In 2011, 2012 and 2013, auditors were able to connect a "rogue" computer and other hardware to the Education Department's networks without being noticed. This same access could allow a hacker to drop into the network environment behind the firewalls and other perimeter security.[55]

In June 2013, when its auditors succeeded with this same "rogue" penetration test, they were even able to access sensitive data stored in the department's networked printers "which could be used in a possible social engineering attack."[56]

Vulnerable user accounts. Hundreds of user accounts employed passwords that had not been changed for over 90 days, and many which had not been changed in over a year, the Inspector General found. The Department also failed to deactivate accounts which had been dormant for 90 days. Both are violations of the Department's own policies, meant to protect against unauthorized access by malicious actors, including hackers and ex-employees.[57] Also, while the Department had distributed authentication tokens to many of its employees – which is required by DHS and OMB guidance – fewer than half were activated for use, the OIG found.[58]

---

[54] "Security Controls for Data Protection over the Virtual Data Center (Plano, TX)," Office of Inspector General, Department of Education, September 2010, p. 2, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2010/a11j0006.pdf, accessed January 13, 2014.

[55] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," Office of Inspector General, Department of Education, November 2012, p. 8, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2013/a11m0003.pdf, accessed January 13, 2014.

[56] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, p. 10. http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

[57] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, pp. 12-13, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

[58] "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," November 2013, p. 24, http://www2.ed.gov/about/offices/list/oig/auditreports/fy2014/a11n0001.pdf, accessed January 13, 2014.

Department of Energy

The many agencies and offices of the sprawling Department of Energy touch nearly every aspect of the nation's energy infrastructure, from generation to transmission and transportation, commercial exchange, research and more. Given how critical its operations are to the national economy and security, one might expect its technology to be more securely protected than most other agencies.

Instead, a close inspection shows the Energy Department's cybersecurity suffers from many of the same basic vulnerabilities and weaknesses found at other federal institutions, which increase the risk that the department's systems could be hacked, and even brought down.[59] Indeed, in January 2013 hackers reportedly compromised 14 servers and 20 workstations, and made off with personal information on hundreds of government and contract employees, and possibly other information.[60] And last July, hackers made off with personal information for 104,000 past and present employees.[61]

Widespread weaknesses at power distribution agency. In October 2012, the Energy IG released an alarming report on cybersecurity weaknesses at the Western Area Power Administration, which markets and delivers wholesale electricity to power millions of homes and businesses through 15 central and western states. "Nearly all" of the 105 computers tested had at least one out-of-date patch; a public-facing server was configured with a default name and password, which "could have allowed an attacker with an Internet connection to obtain unauthorized access to an internal database supporting the electricity scheduling system." What's more, officials at the agency "did not always identify and correct known vulnerabilities." One reason the IG cited: although officials ran vulnerability checks on their IT systems, they ran "less intrusive" scans so as not to slow overall system performance. But those lightweight scans sometimes missed significant weaknesses.[62]

Weak usernames, passwords, and other access controls. The Energy Department's Inspector General found during a 2012 review over a quarter of the sites examined had weak

[59] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 2-3, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[60] Perlroth, Nicole, "Energy Department Is the Latest Victim of an Online Attack," New York Times, February 4, 2013, http://bits.blogs.nytimes.com/2013/02/04/energy-department-is-the-latest-victim-of-an-online-attack/, accessed January 13, 2014.

[61] Goodin, Dan, "How hackers made minced meat out of the Department of Energy networks," Ars Technica, Dec. 16, 2013, http://arstechnica.com/security/2013/12/how-hackers-made-minced-meat-of-department-of-energy-networks/, accessed January 13, 2014.

[62] "Audit Report: Management of Western Area Power Administration's Cyber Security Program," Department of Energy Office of the Inspector General, October 2012, pp. 1-2, http://energy.gov/sites/prod/files/IG-0873.pdf, accessed January 13, 2014.

access controls. The problems included weak usernames and passwords; accounts with improper access; and a server with insufficient security to prevent it from being remotely controlled.[63]

Failure to apply critical patches and updates to software. In 2013, the IG found that 41 percent of the Department's desktop computers auditors examined were running operating systems or applications which had known vulnerabilities that were not patched, even though the software developers had made patches available.[64] In 2012, the IG's team found 41 network servers running operating systems that were no longer supported by the developer, meaning that even when vulnerabilities were discovered in the system, no patch would be made available.[65]

Vulnerable web applications. Several Department web applications had weak security, increasing the risk a hacker could gain unauthorized access to sensitive systems and obtain information, add or change data, or inject flaws or malicious code, the IG found. The weaknesses included the sorts which are considered the most commonly exploited vulnerabilities for web applications.[66]

Unprotected servers. Eleven servers checked by the OIG last year had no password protections or default/weak passwords, meaning an attacker could gain access to the systems, and could use them to attack other systems on the Department's network. One of the unprotected machines the OIG found was a payroll server, which was configured to allow remote access to anyone, without a username or password.[67]

---

[63] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 2-3, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[64] "Evaluation Report: The Department of Energy's Unclassified Cyber Security Program – 2013," Department of Energy Office of the Inspector General, October 2013, http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf, accessed January 13, 2014.

[65] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 3-4, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[66] "Evaluation Report: The Department's Unclassified Cyber Security Program – 2012," Department of Energy Office of the Inspector General, November 2012, pp. 4-5, http://energy.gov/sites/prod/files/IG-0877.pdf, accessed January 13, 2014.

[67] "Evaluation Report: The Department of Energy's Unclassified Cyber Security Program – 2013," Department of Energy Office of the Inspector General, October 2013, http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf, accessed January 13, 2014.

Securities and Exchange Commission

Over the last two decades, financial markets have become increasingly reliant on technology to handle the expanding volume of their business. Today, exchanges like the New York Stock Exchange process millions of trades a day electronically.

In response, the Securities and Exchange Commission (SEC) developed a dedicated team within its Trading and Markets Division to keep an eye on how markets build and manage key trading systems. Among the division's duties is ensuring markets safeguard their systems from hackers and other malicious cyber intruders.

But a 2012 investigation into the team found conduct which did not reflect a concern for security. Team members transmitted sensitive non-public information about major financial institutions using their personal e-mail accounts.[68] They used unencrypted laptops to store sensitive information, in violation of SEC policy — and contravening their own advice to the stock exchanges.[69] Their laptops also lacked antivirus software.[70] The laptops contained "vulnerability assessments and maps and networking diagrams of how to hack into the exchanges," according to one SEC official.[71]

The investigation also found that members of the team took work computers home in order to surf the web, download music and movies, and other personal pursuits.[72] They also appeared to have connected laptops containing sensitive information to unprotected wi-fi networks at public locations like hotels — in at least one reported case, at a convention of computer hackers.[73]

---

[68] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed June 10, 2013; Lynch, Sarah N., "U.S. SEC staffers used govn't computers for personal use," November 9, 2012, http://www.reuters.com/article/2012/11/09/sec-cyber-report-idUSL1E8M9CMI20121109, accessed January 13, 2014.

[69] Lynch, Sarah N., "EXCLUSIVE: SEC left computers vulnerable to cyber attacks," Reuters, November 9, 2012.

[70] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.3, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[71] Lynch, Sarah N., "NYSE hires ex-homeland security chief after SEC security lapse," Reuters, November 16, 2012, http://www.reuters.com/article/2012/11/16/sec-cyber-nyse-idUSL1E8MG95K20121116, accessed January 13, 2014.

[72] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.24, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[73] Lynch, Sarah N., "U.S. SEC staffers used govn't computers for personal use," November 9, 2012, http://www.reuters.com/article/2012/11/09/sec-cyber-report-idUSL1E8M9CMI20121109, accessed January 13, 2014.

The investigation also found that while SEC policy prohibited employees from accessing personal e-mail from web-based sites like Gmail, SEC officials in the division arranged to access an internet-connected network which did not block such sites.[74] These employees also brought in their own personal computers and connected them to the SEC's network.[75] And for a period of several months, the team's network had no firewall or intrusion protection software running.[76] All of these practices increased the risk of introducing viruses and other malware to SEC computers, and potentially compromised sensitive data about the cybersecurity of securities exchanges, not to mention the SEC's own protections.[77]

[74] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.31, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[75] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.35, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[76] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.34, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

[77] "Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets," Securities and Exchange Commission Office of Inspector General, Aug. 30, 2012, p.30, http://www.sec-oig.gov/Reports/OOI/2012/OIG-557.pdf, accessed January 13, 2014.

Statement for the Record

of

THE ELECTRONIC TRANSACTIONS ASSOCIATION

United States Senate

Committee on Homeland Security and Government Affairs

Hearing on "Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"

March 26, 2014

Chairman Carper, Ranking Member Coburn and Members of the Committee, the Electronic Transactions Association (ETA) appreciates the opportunity to submit this statement for the record for the Committee's hearing, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure."

ETA is an international trade association representing companies that offer electronic transaction processing products and services. The purpose of ETA is to help the merchant acquiring industry by providing leadership through education, advocacy, and the exchange of information. ETA's membership spans the breadth of the payments industry, from financial institutions and transaction processors to independent sales organizations and equipment suppliers to merchants. More than 500 companies worldwide are members of ETA.

As the trade association for the payments industry, ETA recognizes the critical importance of data security. With more than 70 percent of consumer spending now done electronically, consumers depend on the security and reliability of payment systems. Consumers prefer electronic payments due to their convenience, efficiency, and low cost, but data theft and cybercrime, if not properly combatted, could cause some consumers to forgo these benefits out of concern about the security of their personal financial information. And if consumers do not have confidence in electronic commerce, then neither will the entrepreneurs and investors who spur financial innovation. Accordingly, the continued development of online commerce and other technology-based sources of economic growth rest on effective data security.

ETA is committed to ensuring that payment systems are fully secure and that customer information is protected. While recent high-profile data breaches remind us of the gravity of the threat posed by cybercriminals, existing data security systems have proven remarkably effective overall. Last year, U.S. payment systems processed more than $5 trillion in payments, and only a small fraction of those payments (less than one tenth of one percent) were fraudulent and consumers had no liability for such fraud. Nevertheless, data security will only be effective if it continues to stay ahead of the always evolving techniques and technologies of criminal enterprises.

Because ETA members are on the front lines of fighting data theft, our members have dedicated significant resources annually to developing secure payment systems. ETA's members have worked with their merchant customers to employ advanced technologies to prevent data theft and the fraudulent use of personal information. Due to these efforts, for example, fraud accounts for less than 6 cents of every $100 of credit and debit card transactions. Even in the relatively small number of cases where fraud does occur, consumers are usually not responsible for those amounts as financial institutions have adopted zero customer liability policies for fraudulent activity.

To further reduce the threat of fraud, ETA members that provide credit and debit cards are also beginning the phase-in of chip smart card technology beginning in 2015. This technology will replace magnetic stripe technology on credit and debit cards with cards containing embedded computer chips, which prevent criminals from producing counterfeit credit and debit cards. The adoption of EMV is a costly undertaking since it requires "point of sale" (POS) terminals to be

updated to handle the new cards, but the investment is expected to yield a significant reduction in the incidents of card fraud and ensure the integrity of payment systems. Our industry is also working hard to deploy other technology solutions to fraud, like tokenization and end-to-end encryption, which hold real promise for thwarting criminal activity against merchants.

ETA recognizes that protecting the personal financial information of consumers is a responsibility shared among payments processors, retailers, and banks. Accordingly, we recently joined with 14 leading retail and financial services trade groups in a partnership aimed at ensuring that our shared infrastructure is secure. This partnership seeks to enhance information sharing to prevent cyber attacks, promote new technologies to stay ahead of increasingly sophisticated threats, and collaborate on comprehensive solutions to threats growing to card-not-present transactions and the mobile environment. ETA believes that such industry collaboration offers the best means for the development of industry standards and innovative solutions to strengthen data security.

With respect to how government can best promote data security, ETA believes that the Federal government has an important role to play in creating a legal and regulatory environment conducive to technological innovation and the efficient and effective protection of consumer information. As Congress considers possible legislative measures to address data security, therefore, ETA would like to offer several recommendations.

1. **Congress should adopt national data breach standards.** ETA believes that a uniform national standard for data breach notification will help make sure consumers

are notified when a security breach puts at risk their personally identifiable information, while minimizing the compliance risks to businesses. Today, payment processors must comply with an ever-changing array of 46 different state laws on data breach. These ambiguous laws unnecessarily increase the cost of data security and confuse consumers with inconsistent rights and responsibilities. A better approach is for a Federal standard that preempts state laws with a clear notification trigger and that provides a reasonable time for notifying consumers following a breach. In addition, Federal data breach legislation should avoid applying duplicative and inconsistent requirements by providing a safe harbor for entities subject to the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, while not subjecting additional entities to these statutes.

2. **Congress should not legislate technology standards.** Since the advent of electronic payments, payments technologies have rapidly evolved to better protect consumer information and further improve the efficiency of electronic payments. While cybercrime has become increasingly complex, payments systems have continued to make the investments in new technology required to keep ahead of criminal efforts. Because future cybercrimes are impossible to predict, payments systems need to have the flexibility to quickly respond to new threats. Thus, Congress should avoid mandating any particular technology standards. Any standard Congress would adopt is likely to be quickly rendered obsolete by new criminal tactics and, therefore, could have the unintended consequence of restricting the ability of payment systems to protect customer information and the integrity of electronic commerce.

3. **A layered approach to data security is the best strategy.** There is no one solution that will prevent every attempt by criminals to steal data. Accordingly, in the same way that banks do not rely solely on vaults to thwart bank robberies, but also utilize in-house security guards, video cameras, and secure facilities, payments systems need to deploy a layered approach to data security. The utilization of multiple defenses - from chip and tokenization to firewalls and encryption - is the best strategy for minimizing data theft. Therefore, ETA recommends that Congress not mandate a particular method of data security.

We want to thank you for the opportunity to present this statement for the record on this important topic. If you have any questions about this statement or the issues discussed, please contact Jason Oxman, President of ETA.

Post-Hearing Questions for the Record
Submitted to Phyllis A. Schneck, Ph.D.
From Senator Tom Coburn

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

Question: Do you see an appropriate role for the Department of Homeland Security (DHS) in regulating cybersecurity within the private sector, for example within critical infrastructure? If so what is that role and what are its appropriate limitations?

Response: The Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience establish a voluntary partnership between the government and private sector to strengthen the cybersecurity and resilience of our critical infrastructure. Trust and partnership underpin our work with the private sector to voluntarily raise the cybersecurity of the Nation.

While the Department of Homeland Security (DHS) does currently administer certain regulatory programs with a cybersecurity component such as the Chemical Facility Anti-Terrorism Standards, DHS is also encouraging participation by the private sector in the Critical Infrastructure Cyber Community or C^3 (pronounced "C Cubed") Voluntary Program and the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Question#:	2
Topic:	CFATS
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: What are the key lessons you think the Department can learn from its management of other voluntary and regulatory programs and apply in its role in helping to secure critical infrastructure against cyber threats? Consider, for example, the Chemical Facility Anti-Terrorism Standards (CFATS) Program in the National Protection and Programs Directorate, and the former Pipeline Security Branch in the Transportation Security Administration.

Response: Based on prior experience working within public-private partnerships, the most important lesson is that trust, transparency, and broad participation are key components to a successful partnership program. One of the main goals of our partnership programs is to provide value by combining disparate pieces of information for deeper understanding of threats and mitigations, and disseminating the information as widely as possible to benefit the greater community. The Critical Infrastructure Cyber Community or C^3 Voluntary Program is a unique public-private partnership that was developed with full stakeholder feedback, including broad swaths of the private sector that contributed to the NIST Cybersecurity Framework. The C^3 Voluntary Program is largely driven by the stakeholders, using a continuous improvement model for developing enhancements. While both the C^3 Voluntary Program and the NIST Cybersecurity Framework will continue to evolve to meet the dynamic challenges of the cyber threats facing our Nation today, trust, transparency, and broad participation continue to be core tenets of the Department's partnership with all its stakeholders.

The critical infrastructure Cyber Information Sharing and Collaboration Program (CISCP) is another voluntary environment for public-private information sharing and collaboration. CISCP pulls together private sector and government analysts and their supervisors in technical threat exchanges and analyst training activities throughout the year. Currently, CISCP has 74 Cooperative Research and Development Agreements for information sharing and collaboration within the program and is in negotiations with approximately 80 additional companies. CISCP analysts have generated approximately 1,600 products during the life of the program, including 25,171 novel indicators of threat. Currently, 22 percent of the information in those products has been based on private sector submitted data and that number is rising.

These programs speak to the success DHS has had in implementing effective voluntary cybersecurity programs, including in the area of critical infrastructure protection.

Question#:	3
Topic:	Windows XP
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you said the Department was on track to migrating all of its systems off of Windows XP by Microsoft's end of support date, April 8, 2014. That date has since passed and Microsoft no longer supports Windows XP. Are there any computers within the DHS that remained on Windows XP after that April 8, 2014?

Response: The total number of devices running Windows XP as of June 2, 2014, in the DHS environment is 6,788. This makes up approximately four percent of DHS IT assets. All DHS Components have submitted aggressive timelines to migrate their remaining assets off of XP as soon as possible. Workstations/assets still running XP after June 2014 are usually only doing so due to Windows 7 incompatibility issues with some legacy applications and hardware issues that must be resolved prior to upgrading operating systems.

Question#:	4
Topic:	zero days
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Do you believe sophisticated and determined adversaries — such as those sponsored by nation-states and transnational organized criminal organizations — present the greatest threat to our cybersecurity? To what extent do you believe these adversaries have access to previously undisclosed vulnerabilities, so called "zero days," and the malicious tools that exploit them?

Response: Sophisticated adversaries sponsored by nation-states and organized crime organizations do pose a prominent threat to the cybersecurity of our critical infrastructure and, thus, our way of life. A critical step in addressing these threats is to evaluate all causes and mitigations using tools such as the Cybersecurity Framework and C^3 Voluntary Program to elevate these discussions to the boardrooms of our private sector partners. Our adversaries have access to funds and capabilities that could threaten our critical infrastructure, economy and way of life if we have not made the appropriate investments in security, resilience, and response capabilities. Each of these threat actors, including insider threats, is capable of exploiting poor security practices, misconfigurations, and vulnerabilities such as 'Heartbleed'.

The Department does observe malicious cyber activity from threat actors who are believed to leverage previously undisclosed vulnerabilities—and use malicious tools that exploit them to engage in a multitude of illegal activities, including intellectual property theft, identity theft, web proliferation of malicious software, web defacements, and denial of service to network resources. Adversaries are becoming increasingly sophisticated in their capabilities to exploit vulnerabilities such as "zero-days."

Ultimately, however, poor information technology management, a lack of effective risk management, and an untrained workforce create huge vulnerabilities. While a zero-day may be the best way to breach a very well-hardened network, the sad reality is that most networks are not well-hardened. In the end, the adversary only needs to find one vulnerability, whether or not it is a zero-day, in order to tilt the playing field in its favor. Resolving that problem takes unified government effort, and private sector and citizen engagement. We must be diligent in protecting against all attack vectors, whether they be zero-day or an alternate form of attack, whether they originate with foreign nation states, organized crime groups, or any other threat actors.

Question#:	5
Topic:	US-CERT
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: On Tuesday, March 18, 2014, US-CERT issued an alert that Google had released a stable channel security update for its popular Chrome internet browser. Yet Google had announced the security fixes four days earlier, following their discovery and reporting in Google's "Pwn2Own" hacker competition, on March 14, 2014. Thus, any Chrome user with auto update disabled, who relied on US-CERT's announcement in this instance, was exposed with known vulnerabilities for at least three days.

Why did US-CERT's alert of the Google Chrome update come four days late and what was the purpose of the alert?

This is not an unusual occurrence — my staff has identified a number of times where US-CERT and ICS-CERT alerts came sometime after the vulnerability had already been publicly announced and widely reported. Is there a purpose that the US-CERT and ICS-CERT alerts are playing that I'm not considering — what is the added value of US-CERT's and ICS-CERT's alerts and advisories, especially those that come days behind the software manufacturer's or other cyber threat reporting services' announcements?

Response: After Google's issuance of the Chrome security fix on March 14, 2014, the United States Computer Emergency Readiness Team (US-CERT) engaged in operational assessments to analyze the security fix, and it solicited input from other partners and stakeholders regarding any adverse impact the fix's application might incur within their environments.

Once analysis was completed and sufficient feedback was received, the National Cybersecurity and Communications Integration Center (NCCIC) team posted the alert regarding the fix mitigation of the Chrome vulnerability.

Although this occurred on March 18, the NCCIC believes it is important to conduct these operational engagements, as doing so ensures alerts and mitigation actions are thorough and provides the best chance of seamless integration into the stakeholder environment that NCCIC serves. The NCCIC will never be faster in releasing information than the vendor that is generating the patch, so that is not a goal of the NCCIC. Instead, the NCCIC vetting ensures that those who receive the NCCIC alert have a higher degree of confidence in that information and are comfortable more rapidly implementing the recommendation. The NCCIC's alerts and advisories also serve as a reference for

Question#:	5
Topic:	US-CERT
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

vulnerability information that can be leveraged by researchers, software developers, and cyber analysts.

Post-Hearing Questions for the Record
Submitted to Phyllis A. Schneck, Ph.D.
From Senator Claire McCaskill

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

Question: If we truly want secure critical infrastructure, what are the reasons to maintain a voluntary approach to the framework?

Response: Executive Order 13636 and PPD-21 establish a voluntary partnership between the government and private sector to strengthen the cybersecurity and resilience of our critical infrastructure. A voluntary approach can improve information-sharing and maintain high trust without fear of repercussion or enforcement dynamics. It can also preserve freedom-of-action for private sector technologists to come up with innovative ways to address cybersecurity threats.

The government recognizes that for-profit private sector organizations regularly manage risk in their ordinary course of business. Executive Order 13636 and PPD-21 initiatives, such as the NIST Cybersecurity Framework and the Department's C3 Voluntary Program, are designed to assist critical infrastructure entities as they build cybersecurity into their risk management approaches. A voluntary approach to cybersecurity will support private sector efforts to mature their risk management practices from within. This voluntary approach will also help enable markets to drive better cybersecurity and infrastructure resilience through new innovation. For example, a recent Request for Information released under the C3 Voluntary Program encourages companies to develop cybersecurity technologies that are tailored towards being more available and affordable to often under-resourced small- and medium-sized businesses. DHS understands that trust and partnership and leaving room for innovation are necessary to working with the private sector to raise the cybersecurity of the Nation.

Question#:	7
Topic:	limiting liability 1
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, during a discussion on limiting liability for companies that share information with each other and with the federal government, Sen. Coburn discussed a lack of trust in the private sector on the part of the federal government "to do what's best for the country as a whole." The result of the lack of trust is the government's unwillingness to grant broad immunity from liability to the private sector for sharing information about cyber threats. In his estimation, the vast majority of the public wants to do the right thing.

It could also be argued, however, that the vast majority of the federal government also wants to do the right thing, and the private sector's lack of trust in the federal government prevents mandatory information sharing which hurts our national security.

What do you think of these two positions?

Response: One of NPPD's strongest tools in our efforts to increase the security and resilience of cyberspace is our ability to share and receive cyber threat information. Building the trust necessary to have reliable relationships with private sector and Federal partners is among our most important work. However, we have run into situations in which partners have chosen not to share information with us despite the possible protection that information could offer others. Companies often are concerned that if knowledge of a cyber incident becomes public it will cause serious damage to their reputation and could harm others in a sector, for example, by affecting stock prices. In the absence of clarity, companies sometimes choose to err on the side of protecting their shareholders and the company, even if it is not in the best interest of the security community, or the best possible course of action for their customers. These are difficult decisions that are not made by a lack of concern for the security of others. Rather in many cases, corporate governance drives the decision to withhold information when there is a lack of clarity on liability, and uncertainty about the government's ability to keep cyber incident information in confidence. Unfortunately, the end result is that the greater community lacks potentially helpful information that could save others from harm, and the affected critical infrastructure entity itself may not be able to effectively address the cyber threat.

To alleviate these fears, the Department can currently offer protection from disclosure of sensitive information under the Protected Critical Infrastructure Information Act, although that Act only protects information provided to the Government, and does not

Question#:	7
Topic:	limiting liability 1
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

protect communications such as technical assistance or advice from the Government to the critical infrastructure entity. The Administration is also taking steps to address this problem by clarifying anti-trust rules concerning the sharing of cyber threat information and expanding outreach efforts through the C^3 Voluntary Program.

Question#:	8
Topic:	cost-sharing
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, Sen. Coburn noted that it is in companies' best interest to maximize their cybersecurity. But companies also want to maximize their profits and minimize their costs. They will weigh their liability and the costs to their bottom line of a cyber-attack against the cost of improving their cybersecurity.

How, if at all, might the profit motive of companies and companies' involvement in the development of cybersecurity policies and requirements result in cost and burden shifting of securing private assets that are also critical national infrastructure components to the federal government?

To what degree has cost-sharing among the private and public sectors been considered when developing cyber-security, including both the cost to increase security before an attack and the costs to repair any damaged infrastructure after an attack?

Response: While the Department agrees that the best incentive is when companies are motivated to mitigate their own risk, as they identify it, EO 13636 also directed the Departments of Commerce, Homeland Security, and Treasury to propose further incentives to drive better security practices, encourage participation in the Department's voluntary program, and promote use of the NIST Cybersecurity Framework. Eight of those incentives are under advisement now. It is a complex landscape in which private actors are legally obligated to prioritize their own bottom lines, but moral and social codes ask them to share information that helps others protect themselves and to invest heavily in security so that there is shared social benefit. We are working with other agencies, private sector entities, and the best and brightest thinkers in the field to address these sometimes-competing interests in the most efficient way.

This voluntary approach will also help enable markets to drive better cybersecurity and infrastructure resilience through new innovation. For example, a recent Request for Information released under the C^3 Voluntary Program encourages companies to develop cybersecurity technologies that are tailored towards being more available and affordable to often under-resourced small- and medium-sized businesses.

Question#:	9
Topic:	limiting liability 2
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: During the hearing, there was a lot of discussion regarding limiting liability in order to improve information sharing. However, it seems to me that the discussion at the hearing ignored the incentives that liability provides not to act in a negligent manner. We must certainly do all that we can to ensure that the private sector's incentives to share information align with the federal government's incentives to provide broad protections against cyber threats, but I think that some sort of liability may have a role to play in aligning incentives.

Do you agree? Why or why not?

Response: The Administration's position is that the government should work to further clarify laws regarding cyber threat information sharing and that any new liability protection should be narrowly targeted and work to strengthen privacy and civil liberties protections already in place. Additionally, the Department does not want to take away from existing consumer protections. The question of whether and how to best employ liability protection is complex and there is no one right answer.

We believe that companies are incentivized to protect their brand, infrastructure, and digital property. And under the C^3 Voluntary Program, DHS is working to make tools and resources available that allow companies to strengthen their cybersecurity posture. Our mission is to promote cybersecurity, and while we share your interest in liability protection questions, we strive to do the best work possible in the current environment.

I spent my entire career in the private sector and, as was stated earlier, I believe many companies want to act in the best interests of our Nation and the security community.

Question#:	10
Topic:	catch the bad guys
Hearing:	Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: During the second panel of the hearing, Mr. Steven Chabinsky, Chief Risk Officer, CrowdStrike, Inc. discussed the role of deterrence, and Mr. Doug Johnson, Vice Chairman, Financial Services Sector Coordinating Council, noted that it is the role of government to "catch the bad guys."

Do you believe that this attitude shifts the burden of paying for cybersecurity onto the federal government and away from the private sector?

Response: Cybersecurity is a shared responsibility, and fear of criminal repercussion is not the only disincentive to bad behavior. Government and the private sector can collaboratively raise the cost to malicious actors of their bad behavior, whether through criminal prosecution, vulnerability reduction, consequence mitigation, or a combination thereof. The DHS mission spans protection, prevention, mitigation, response, and recovery. We often use the locked door analogy to describe the role of government when it comes to cyber: companies have the responsibility to buy the locks for their house doors, while the police have the responsibility to take the cyber criminals off the street. That being said, companies are in the best position to assess what level of security they apply to various parts of their organizations, and they have their own incentive to deter theft and intrusion. In NPPD, we often share threat and vulnerability warnings and associated mitigation strategies as well as analyses of potential consequences. These can be used by private sector companies in their risk calculus and security decisions; however, we partner closely with the U.S. Secret Service, U.S. Immigration and Customs Enforcement's Homeland Security Investigations, and the Federal Bureau of Investigation to ensure we provide whatever support we can to law enforcement's actions in disrupting cyber criminals.

Post-Hearing Questions for the Record
Submitted to Ms. Donna Dodson
From Senator Tom Coburn

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

1. **What are the National Institute of Standards and Technology's (NIST) future plans regarding the framework?**

    a. **Does NIST plan to continue to update the Framework?**

Answer:
Yes, NIST plans to work with industry, the Department of Homeland Security (DHS), and other government agencies to support and improve the Framework. The Framework is a living document that will evolve based on industry feedback, and best practices, including changes in the threat environment, as well as changes in information technology and cybersecurity capabilities.

    b. **How else will NIST remain involved in the process?**

Answer:
As noted in our companion publication, "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," NIST will continue to serve as a convener and coordinator to work with industry, DHS, and other government agencies to help organizations understand, use and improve the Framework. In addition, Executive Order 13636 called for the Framework to "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations." Based on stakeholder input, NIST continues to work with stakeholders on high-priority areas for development, alignment, and collaboration that will inform future revisions of the Framework.

As the Framework evolves, NIST will lead discussions of models for future governance of the Framework, such as potential transfer of the convener role to a non-government organization, while maintaining NIST involvement.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 16, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

Critical Infrastructure Protection: GAO Response to Posthearing Questions for the Record

Dear Mr. Chairman:

On March 26, 2014, we testified before your committee on observations on key factors that are important to DHS's implementation of its partnership approach to protect critical infrastructure from cyber attacks.[1] You requested that we provide additional information on a number of posthearing questions. The questions and our answers are provided in the enclosure. The responses are based on work associated with previously issued GAO products. If you have any questions about this report or need additional information, please contact me at (202) 512-9610 or CaldwellS@gao.gov.

Sincerely yours,

Stephen L. Caldwell
Director
Homeland Security and Justice Issues

Enclosure

[1]GAO, *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach*, GAO-14-464T (Washington, D.C.: Mar. 26, 2014).

Enclosure

Questions from the Honorable Thomas R. Carper

1. **What is the Department of Homeland Security's (DHS) track record as a regulator of critical infrastructure? Where has DHS been effective and where can the Department improve in regulating chemical facilities under its CFATS program?**

   Our prior work on DHS's role as a regulator of critical infrastructure—for example, our maritime security work covering DHS's responsibility to improve various parts of the maritime transportation system, including related critical infrastructure,[2] and management of its Chemical Facilities Anti-Terrorism Standards (CFATS)[3] program—has shown that DHS has a mixed track record.

   As one example, we have previously reported that, although DHS and the Coast Guard have made substantial progress in implementing initiatives and programs to enhance maritime security since 2002, they have also encountered challenges.[4] In general, GAO's work on maritime security programs falls under four areas: (1) security planning, (2) port facility and vessel security, (3) maritime domain awareness and information sharing, and (4) international supply chain security. DHS has, among other things, developed various maritime security programs and strategies and has implemented and exercised security plans. For example, to enhance the security of U.S. ports, the Coast Guard has implemented programs to conduct annual inspections of port facilities. Although DHS and its components have made substantial progress in enhancing maritime security, they have also encountered challenges in implementing related initiatives and programs in the areas of (1) program management and implementation; (2) partnerships and collaboration; (3) resources, funding, and sustainability; and (4) performance measures. For example, in a February 2012 report, we found that the Coast Guard faced collaboration challenges when developing and implementing its information management system for enhancing information sharing with key federal, state, and local law enforcement agencies because it did not systematically solicit input from these stakeholders.[5] We recommended that the Coast Guard implement a more systematic process to solicit and incorporate port partner input and, as of May 16, 2014, this recommendation remains open.

---

[2]Enacted in 2002, the Maritime Transportation Security Act of 2002 (MTSA) required a wide range of security improvements to various parts of the maritime transportation system including critical infrastructure. See Pub. L. No. 107-295, 116 Stat. 2064. DHS is the lead federal department responsible for implementing MTSA and it relies on its component agencies, such as the Coast Guard to help implement the act. The Coast Guard is responsible for U.S. maritime security interests.

[3]As required by the DHS appropriations act for fiscal year 2007, DHS issued regulations that establish standards for the security of high-risk chemical facilities. See Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006). DHS established the CFATS program in 2007 to assess the risk posed by these facilities and inspect the facilities to ensure compliance with DHS standards. DHS places these high-risk facilities in risk-based tiers and is to conduct inspections after it approves facility security plans.

[4]GAO, *Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act*, GAO-12-1009T (Washington, D.C.: Sept. 11, 2012).

[5]GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*, GAO-12-202 (Washington, D.C.: Feb. 13, 2012).

As we have previously reported in February 2014, DHS has also experienced some challenges in regulating high-risk chemical facilities[6] under the CFATS program; however, the department has a number of efforts underway to address these challenges and in particular in the areas of (1) identifying facilities that are covered by the program, (2) assessing risk and prioritizing facilities, (3) reviewing and approving facility security plans, and (4) inspecting facilities to ensure compliance with security regulations.[7] Regarding identifying facilities, DHS has begun to work with other agencies to identify facilities that should have reported their chemical holdings to CFATS, but may not have done so. Regarding assessing risk and prioritizing facilities, DHS has begun to enhance its ability to assess risks and prioritize facilities. Regarding reviewing security plans, DHS has also begun to take action to speed up its reviews of facility security plans. Regarding inspecting facilities to verify compliance, DHS reported it had begun to perform inspections at facilities to ensure compliance with their site security plans. Given this recent development, we have not yet reviewed this aspect of the program.

2. What is DHS's track record with information sharing in the physical security world?

Our prior work has shown that while DHS continues to share information in the physical security world, opportunities exist for increased information sharing to enhance the security of critical infrastructure in the maritime domain and the security of other critical infrastructure.

With regard to information sharing to enhance the security of critical infrastructure in the maritime domain, we have previously reported that the Coast Guard is responsible for establishing interagency operations centers (IOC) in response to provisions of the Security and Accountability For Every Port Act of 2006 (SAFE Port Act).[8] IOCs are designed to, among other things, share maritime information with the Coast Guard's federal, state, and local port partners, such as through the use of enhanced physical facilities and sensors to establish radar and camera coverage throughout ports.[9] To facilitate IOCs, the Coast Guard is implementing an information management and sharing system called WatchKeeper. In a February 2012 report assessing the status of IOC and WatchKeeper implementation, we found that the Coast Guard is continuing its efforts to establish IOCs at 35 locations and share maritime domain awareness information with its port partners.[10] However, we found that there were factors that jeopardized the capability of such centers in meeting their purpose to improve information sharing. These included the lack of a documented process that describes how the Coast Guard will obtain and incorporate stakeholder feedback into the development of future WatchKeeper requirements. We recommended that the Coast

[6]According to DHS, a high-risk chemical facility is one that, in the discretion of the Secretary of Homeland Security, presents a high risk of significant adverse consequences for human life or health, national security, or critical economic assets if subjected to a terrorist attack, compromise, infiltration, or exploitation. 6 C.F.R. § 27.105.

[7]GAO, *Critical Infrastructure Protection: Observations on DHS Efforts to Identify, Prioritize, Assess, and Inspect Chemical Facilities*, GAO-14-365T (Washington, D.C.: Feb. 27, 2014).

[8]See Pub. L. No. 109-347, § 108, 120 Stat. 1884, 1892-93 (2006).

[9] Port partners include federal agencies and armed services such as U.S. Customs and Border Protection (CBP), U.S. Immigration and Custom Enforcement (ICE), and the U.S. Navy; state and local organizations such as port authorities, state law enforcement, and local law enforcement; and private sector organizations such as marine exchanges.

[10]GAO-12-202.

Guard develop, document, and implement a process to obtain and incorporate port partner input into the development of future WatchKeeper requirements. In November 2013, Coast Guard officials stated that the President's Fiscal Year 2013 Budget did not provide additional resources for these efforts and that no new funding was requested for the project in the President's Fiscal Year 2014 Budget. Noting that funding situations can change, this recommendation remains open.

With regard to information sharing to enhance the security of other critical infrastructure, our testimony statement discusses and provides examples from prior work of various areas where opportunities exist for DHS to further enhance information sharing in the physical security world.[11] Specifically, our prior work has identified multiple examples in the following areas: (1) recognizing and addressing barriers to sharing information, (2) sharing the results of DHS assessments with industry and other stakeholders, and (3) measuring and evaluating the performance of DHS's partnership efforts. For example, In April 2013, we examined DHS's CFATS program and assessed, among other things, the extent to which DHS has communicated and worked with owners and operators to improve security.[12] Specifically, we reported that DHS had increased its efforts to communicate and work with industry owners and operators to help them enhance security at their facilities since 2007. We found that as part of their outreach program, DHS consulted with external stakeholders, such as private industry and state and local government officials to discuss issues that affect the program and facility owners and operators. However, despite increasing its efforts to communicate with industry owners and operators, we also found that DHS had an opportunity to obtain systematic feedback on its outreach. We recommended that DHS explore opportunities and take action to systematically solicit and document feedback on facility outreach. DHS concurred with this recommendation and has actions underway to explore such opportunities to make CFATS-related outreach efforts more effective for all stakeholders.

a. How well has DHS shared useful, timely information from its surveys and assessments with critical infrastructure? With state and local governments?

We have not reported comprehensively on DHS's efforts to share useful, timely information from its surveys and assessments with critical infrastructure stakeholders. However, our prior work provides some examples of progress made and where opportunities exist for DHS to increase the timely sharing of information on the results of its surveys and security assessments with stakeholders at various levels, from individual asset owners and state and local governments to sector-specific agencies and regional partners. For example, in a May 2012 report, we assessed, among other things, the extent to which DHS had shared the results of these surveys and assessments with asset owners or operators.[13] We found that DHS does share the results of security surveys and vulnerability assessments with asset owners or operators. However, we also found that the usefulness of security survey and vulnerability assessment results could be enhanced by the timely delivery of these products to the owners and operators and that the inability to deliver these products in a timely manner could undermine the

[11]GAO-14-464T.

[12]GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: Apr. 5, 2013).

[13]GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

relationship DHS was attempting to develop with these industry partners. Specifically, we reported that, based on DHS data from fiscal year 2011, DHS was late meeting its (1) 30-day time frame—as required by DHS guidance—for delivering the results of its security surveys 60 percent of the time and (2) 60-day time frame—expected by DHS managers for delivering the results of its vulnerability assessments—in 84 percent of the instances. DHS officials acknowledged the late delivery of survey and assessment results and said they were working to improve processes and protocols. However, DHS had not established a plan with time frames and milestones for managing this effort consistent with standards for project management. We recommended, and DHS concurred, that it develop time frames and specific milestones for managing its efforts to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners and operators. DHS stated that, among other things, it deployed a web-based information-sharing system for facility-level information in February 2013, which, according to DHS, has since resulted in a significant drop in overdue deliveries.

Our work has also highlighted challenges DHS has experienced in its efforts to share information from its surveys and assessments. For example, in a September 2010 report assessing, among other things, the extent to which DHS is positioned to disseminate information it gathers on resiliency practices to critical infrastructure asset owners and operators, we found that DHS faces barriers to doing so.[14] Specifically, we reported that DHS does share some information on vulnerabilities and potential protective measures (such as critical infrastructure vulnerabilities DHS has identified and corresponding steps that the asset owners and operators and take to mitigate these vulnerabilities) with asset owners and operators and others including state and local officials ,generally on a case-by-case basis, after it has completed vulnerability assessments at critical infrastructure facilities. However, DHS officials stated that, given the voluntary nature of the critical infrastructure partnership, DHS should not be viewed as identifying and promoting standards that have to be adopted and expressed concerns about sharing proprietary information.[15] Also, according to DHS officials, the need for and the emphasis on resiliency can vary across different types of facilities, depending on the nature of the facility.

While recognizing that DHS would face challenges in disseminating information about resiliency practices within and across sectors, especially since resiliency can mean different things to different sectors, we concluded in our September 2010 report that DHS, as the primary federal agency responsible for coordinating and enhancing the protection and resiliency of critical infrastructure, is uniquely positioned to disseminate this information. We recommended that DHS determine the feasibility of overcoming these barriers and develop an approach for disseminating information on resiliency practices to critical infrastructure owners and operators within and across sectors. In response, DHS agreed to expand the distribution of resiliency products to critical infrastructure stakeholders. In November 2013, DHS reported that as DHS's collection of

[14]GAO, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, GAO-10-772 (Washington, D.C.: Sept. 23, 2010).

[15]Most of the nation's critical infrastructure is privately owned and does not fall within the regulatory scope of DHS or its components. As a result, a fundamental component of DHS's efforts to protect and secure our nation's critical infrastructure is partnerships among public and private stakeholders, with an emphasis on collaboration, partnering, and voluntary information sharing among DHS and private sector asset owners and operators, and state, local, and tribal governments.

data and knowledge has grown through assessments and other activities, it has begun to expand the distribution of resilience products to critical infrastructure partners to provide information on characteristics of critical infrastructure resilience. As a result, this recommendation has been closed as implemented.

b. Does DHS have an effective process for following up with recommendations and risks identified in its multitude of different assessment products?

We have not reported comprehensively on DHS's processes for following up with recommendations and risks identified in its multitude of different assessment products. However, our prior work provides some examples of where we have assessed some of DHS's efforts to follow up on recommendations and risks identified in its assessment products and generally highlights areas where DHS can improve upon its processes for (1) collecting and evaluating information on the impact of DHS's surveys and assessments on industry's decisions to make, or not make, security enhancements; (2) measuring the effectiveness of regional-level assessments; and (3) obtaining and assessing feedback from critical infrastructure stakeholders, such as industry partners.[16] For example, in our July 2013 report examining DHS's management of its Regional Resiliency Assessment Program (RRAP)—a voluntary program intended to assess regional resilience of critical infrastructure by analyzing a region's ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions—we found that DHS had taken action to measure efforts to enhance security and resilience among facilities that participated in these regional-level assessments, but faced challenges in measuring the results associated with these projects.[17] We concluded that DHS could better position itself to gain insights into projects' effects if it were to develop a mechanism to compare facilities that have participated in a RRAP project with those that have not, thus establishing building blocks for measuring its efforts to conduct RRAP projects. DHS concurred with our recommendation and reported that it had actions under way to review alternatives, including possibly revising its security survey and vulnerability assessment follow-up tool, to address this issue. In September 2013, DHS reported that this review will be completed and the agency will begin tracking results by September 2014.

3. To what extent do you see Congress as part of the larger public-private partnership in critical infrastructure protection?

Our prior work has shown that Congress serves a vital role as part of the larger public-private partnerships for critical infrastructure protection through its continued oversight efforts. Congress provides funding, policy guidance, and oversight by mandating legislative reporting requirements for agencies such as DHS, holding oversight hearings, and requesting GAO reports that look at these issues. For example, congressional reporting requirements have assisted in congressional oversight and work to inform funding decisions that can directly affect DHS partnership and protection efforts. Moreover, multiple congressional hearings on critical infrastructure protection have provided a forum for public and private partners to present issues and areas for discussion. Furthermore, at the request

[16]GAO-14-464T, 14-17.

[17]GAO, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*, GAO-13-616 (Washington, D.C.: July 30, 2013).

of Congress, GAO analysis led to identifying challenges and issues relating to DHS critical infrastructure protection efforts, as well as to highlight areas of growth and development.

4. **In your reports on critical infrastructure protection, you commented not only on the DHS partnership approach, but also statutory requirements for DHS to report to Congress on aspects of the partnership. Has DHS met its reporting requirements to Congress on such matters? In your response, please cite examples, including details for each.**

   We have not reported comprehensively on DHS's congressional reporting requirements regarding critical infrastructure protection. However, our prior work has shown that DHS has not met some of its reporting requirements to Congress regarding critical infrastructure protection. DHS has statutory requirements to keep Congress informed of its public-private partnership efforts to protect the nation's critical infrastructure, and these reporting requirements can assist in congressional oversight and funding decisions that can directly affect DHS efforts. The following provide some examples where we found that DHS has not consistently met these requirements:

   - **Required report on streamlining the DHS partnership model did not address required elements.** In November 2013, we reported that the National Protection and Programs Directorate (NPPD) was directed in 2011 to provide the Senate and House Appropriation Committees with a report on the results of a review to streamline the processes for coordination and information sharing with industry partners, and that GAO was to conduct an evaluation of the effort.[18] We found that DHS's response, provided to the Senate and House Appropriation Committees in August 2013, did not provide information about NPPD efforts to streamline the processes for coordination and information sharing. NPPD officials agreed that the submission provided by DHS did not discuss NPPD efforts to streamline the processes for coordination and information sharing with industry partners and that the submission was not responsive to congressional concerns. In its written comments, DHS concurred that the report provided to the Senate and House Appropriation Committees fell short of fully capturing and describing its streamlining efforts. In its response, DHS provided additional information on actions the agency had taken, was taking, or planned to take to provide a framework for streamlining methods and processes for coordinating information sharing with industry partners.

   - **Required annual report on critical infrastructure priorities not provided.** In March 2013, we reported that DHS is required to report annually to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on, among other things, any significant challenges in compiling the National Critical Infrastructure Prioritization Program (NCIPP) database or list[19] and, if appropriate, the extent to which either had been used to allocate federal funds to prevent, reduce, mitigate, or respond to acts of terrorism.[20] We found that, although DHS was able to compile this information for fiscal

[18]GAO, *Critical Infrastructure: Assessment of the Department of Homeland Security's Report on the Results of Its Critical Infrastructure Partnership Streamlining Efforts*, GAO-14-100R (Washington, D.C.: November 18, 2013).

[19]The NCIPP database or list identifies and prioritizes a list of nationally significant critical infrastructure each year.

[20]GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 (Washington, D.C.: Mar. 25, 2013).

years 2008 through 2011, DHS could not verify that it was delivered to the requisite congressional committees because its document tracking system did not contain a record to confirm that the transaction actually occurred. In addition, staff from both committees could not find evidence that DHS had reported on these requirements. We reported that, absent an approach to verify the delivery of the statutorily required reports, DHS could not ensure that it had provided the committees with the necessary information in a timely manner. We recommended that DHS develop an approach to verify the delivery of the statutorily required annual reports on the database and list to the requisite congressional committees. In response to this recommendation, DHS reported that it, among other things, finalized a standard operating procedure (SOP) for tracking the delivery of annual reports on the database and the list in July 2013 and that the 2011-2012 report was subsequently delivered to Congress in August 2013.

- **Required report on infrastructure cost-benefit analysis not provided.** In June 2009, we reported that Congress had directed DHS to provide the Senate and House Appropriation Committees with a report on whether the department should require private sector entities to provide DHS with existing information about their security measures and vulnerabilities in order to improve the department's ability to evaluate critical infrastructure protection nationwide.[21] This report was to include an analysis of the costs to the private sector and DHS for implementing such a requirement and the benefits of obtaining the information. We noted that this direction was consistent with concerns raised by the House Appropriations Committee about DHS's progress conducting vulnerability assessments for critical infrastructure facilities generally, and security measures at chemical facilities in particular. We reported that although the report was completed in 2005 and updated in 2007, the report was never delivered to the Senate and House Appropriation Committees.

441217

[21]GAO, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, GAO-09-654R (Washington, D.C.: June 26, 2009).

United States Senate Committee on Homeland Security and Governmental Affairs
"Strengthening Public-Private Partnerships to Reduce Cyber Risks
to Our Nation's Critical Infrastructure"
Hearing Date: March 26, 2014

Response to Post-Hearing Questions for the Record
From Senator Tom Coburn

Submitted by Mr. Steven Chabinsky
(in his personal capacity)

1. **Do you believe we can defend against sophisticated and determined cyber adversaries through vulnerability mitigation alone?**

   Although vulnerability mitigation must remain a core component of cybersecurity, it is not sufficient to defend against sophisticated and determined adversaries. This is true as well in other security settings. Vulnerability mitigation tends to be most effective as a primary security strategy only within controlled, static, and isolated environments (such as bunkers, to include missile silos). However, vulnerability mitigation security efforts lose their efficacy over time in environments that are dynamic, interoperable, and where there is substantial freedom of movement. In those environments, which include the Internet, threat deterrent strategies have proven most effective and efficient over time.

2. **How likely are sophisticated and determined cyber adversaries — state sponsored or criminal organizations — to have access to previously undisclosed vulnerabilities, so called "zero days," and the malicious tools that exploit them?**

   It is inevitable that sophisticated and determined cyber adversaries always will have access to previously undisclosed vulnerabilities together with the malicious tools to exploit them. This is a function of a number of factors, to include the complexities, interconnectedness, and constant changes that are made within and between commonly used software and hardware components. Research indicates that, at any given time, there likely are no fewer than 50 zero days that could be used to compromise commonly used products.

   Do you believe sophisticated and determined cyber adversaries with access to zero days pose a serious threat to our nation's cybersecurity?

   Sophisticated and determined cyber adversaries with access to zero days pose a serious threat to our nation's economic security, homeland security, and national security. As we grow increasingly reliant upon vulnerable technologies across all of our critical infrastructure and the growing "Internet of Things," there is an increasing risk of substantial harm to the confidentiality of information, and the integrity and availability of information and information systems that can impact significant aspects of our military preparedness as well as human health and safety. Indeed, at this very moment, attackers

could be pre-positioned to manipulate networks at will and already may be doing so in ways we might not detect for years to come.

a. One of the key cybersecurity programs proposed by the Department of Homeland Security (DHS) to reduce the nation's cyber risk is Einstein, a threat-signature based intrusion detection and prevention system for unclassified federal networks. A similar DHS system, called Enhanced Cybersecurity Services, would provide the same threat signatures used by Einstein to protect privately owned and operated critical infrastructure. Anti-virus software also generally employ threat signatures as the first step to detecting and stopping malicious software. To what extent do those sorts of signature based systems protect against zero day attacks, if at all?

Anti-virus products typically rely on signatures of known malicious programs as well as on heuristics of anomalous activity. Unfortunately, the "known signature" based detection component will not detect or stop zero day attacks. Heuristic analytic capabilities may protect against zero day attacks, but traditionally have not done an effective job. Rather, heuristic systems typically have had low detection rates for new malware coupled with high false positive rates, making them ineffective in practice. Significantly, adversaries routinely test their attack methodologies against common anti-virus products until they are able to evade one or more of them.

b. Other common cybersecurity protections and mitigation systems include firewalls and continuous monitoring for known vulnerabilities (which DHS has proposed through its Continuous Diagnostics and Mitigation program and Continuous Monitoring as a Service). Generally, how effective are those sorts of defenses against zero day attacks?

The concept of Continuous Diagnostics and Mitigation is sound, so long as it is not limited to a review of vulnerabilities. Although continuous monitoring for vulnerabilities is not an effective defense against zero day attacks, continuous monitoring for threat activities can be a very effective method to detect and prevent zero day attacks. The new breed of cybersecurity technologies therefore focus on instantly detecting and responding to adversary behaviors and effects at the endpoint rather than solely at the perimeter -- to include instant detection and response to an adversary's malicious code execution, actions taken to avoid detection, attempts to gain persistence on a computer, establishing network connectivity to allow adversarial command and control, and lateral movement between systems to escalate user privileges.

3. **In your testimony, you posited that deterrence could be a more effective strategy to reduce cyber risk than vulnerability mitigation. What do you see as the key factors necessary for deterring cyber adversaries, both those acting at the behest of nation-states and those working within transnational organized criminal organizations?**

The key factors necessary for deterring cyber adversaries are (1) instant detection, (2) identification of the responsible actor, and (3) enforcement of a credible penalty. Each of these aspects deserves our in-depth review, culminating with an international framework, that takes advantage of the full spectrum of private sector and governmental capabilities, resources, and authorities, and provides a credible path forward as a matter of technology, economics, law, and policy. Achieving adequate cybersecurity also may require a more sophisticated and discrete approach than we have taken to date. In the area of critical infrastructure protection, we would do well to focus first on discovering and resolving threat deterrent models where security is paramount and privacy considerations may be lower (for example, focusing on the technologies, laws, norms, and policies necessary to achieve intrusion detection, hacker identification, and sufficient penalties – or incentives -- to deter and immediately address intrusions into industrial control systems). Achieving cyber threat deterrence is necessary and achievable, but will require sustained, multi-disciplinary efforts combined with strong leadership.

4. **Given your past work at the Federal Bureau of Investigation and in the private sector, as well as your experience with federal initiatives to encourage information sharing between the government and private sector, what are your recommendations to improve cybersecurity information sharing between the public and private sectors?**

In order to improve cybersecurity information sharing between the public and private sectors, it is helpful to consider what has been working and what has not been working over the past 15 years. Information sharing partnerships (regardless of their public/private composition) that have not worked well tend to suffer from a common problem: they are more focused on the mechanics and quantity of sharing than they are on establishing and measuring the tactical and strategic objectives and outcomes of their efforts. There is little to no value in pushing vast quantities of data around communities, even if carefully structured, unless a plan exists demonstrating that it is the most effective and efficient approoch for achieving a relevant outcome. In this regard, I recoll once being told that a number of companies had agreed to a plan for sharing all of their intrusion prevention data with one onother. I asked why, and the response was, "well, we've never managed to agree on that level of sharing before." I followed up by asking what the companies were going to do with all of that data. The response was, "we're going to see if it can be used against botnets." I asked whether there was anything about the noture or amount of data or the types of companies sharing the data that suggested it was useful either as a short-term or a long-term approach to botnet mitigation. The response was, "I'm not sure, I'll go ask." I never heard back. This is just one of many examples I have witnessed over the years in which well meaning information sharing partners focus more on describing and measuring the "who, what, when, and how" of sharing than the "why?" Information sharing cannot be ollowed to become a numbers game in which the passage of large

quantities of "indicators and warning" is viewed in and of itself as a metric of success regardless of cost and outcomes.

In contrast, information sharing partnerships that work tend to be collaborative endeavors that (1) identify and prioritize security issues, (2) determine whether data sharing is helpful to resolve the problem, and if so, (3) seek to determine and then acquire the minimal level of sharing necessary for maximum impact, (4) provide members with a plan of action upon receipt of the shared information, oftentimes resulting in coordinated action, and (5) measure short term and long term outcomes of the approach, course-correcting as necessary. Mature security partnerships also recognize that positive tactical outcomes can result in negative strategic outcomes (winning the battle but losing the war) if the approach cannot scale to meet the exponential growth of the threat or best efforts actually result in negative returns by encouraging threat actors collectively to up their game.

In response to the more specific aspect of the question as it relates to cybersecurity information sharing between the public and private sectors, we must ensure a coordinated approach as to the information's timeliness, uniqueness, relevance, and planned use, all backed by definitive measures of how the approach is faring over time relative to the nature and level of threat actor success. Doing so requires collaboration, of which information sharing typically is only a small part.

/////

Submitted on May 16, 2014

Post-Hearing Questions for the Record
Submitted to Mr. Doug Johnson
From Senator Tom Coburn

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

1. **How long has the Financial Services Information Sharing and Analysis Center (FS-ISAC) had a representative on the floor of the National Cybersecurity and Communications Integration Center (NCCIC)?**

   The FS-ISAC has had access to the NCCIC floor since June of 2011.

2. **What challenges did the FS-ISAC encounter in getting a representative on the floor of the NCCIC?**

   The FS-ISAC hired a full-time representative to the NCCIC in June of 2012. Despite the fact that the hire was formerly with DHS Intelligence and Analysis, had had access to the NCCIC floor previously and held a TS/SCI level clearance, the ISAC was not able to get him on the floor until October of 2013.

3. **How much did it cost for the FS-ISAC to gain entry to the NCCIC?**

   The FS-ISAC hired and paid a salary for a representative to the floor during the period from June 2012 until access was finally granted in October 2013. There were also a minimum of 2 hours spent per week making requests, completing paperwork and generally attempting to get some movement on getting the representative access to the NCCIC. The FS-ISAC also retained services on a consultative basis to help expedite the clearance recognition process.

4. **What do you see as the key barriers to effective information sharing between the federal government and the private sector? How do you think we can strengthen information sharing between DHS, your sector, and the other ISACs?**

   The FS-ISAC believes in the concept of the NCCIC. In theory the NCCIC serves as a fusion point between government/the intelligence community and the Critical Infrastructure (CI) with the ISACs representing the various CI.

   Support the Various ISACs
   The ISACS should be recognized and supported as gateways to and from the various CI sectors. In the financial sector, Treasury and the FBIIC have been very supportive of the FS-ISAC and have strongly encouraged owner/operator support and membership in the ISAC. DHS should likewise, as SSA for 9 of the 16 CI sectors, support the ISACs in the sectors it serves.

Streamline the Clearance Process
DHS should develop a single private sector clearance process. DHS Infrastructure Protection (IP) has a Private Sector Clearance Program that provides up to a Secret level clearance. Under the DHS CISCP and the CRADA process there is supposed to be a process to get cleared to TS but neither of these processes seems to be working well at this time. There are a number of ISACs with personnel who hold TS clearance levels who have been in limbo since the program started several years ago. Currently just 5 out of 17 ISACs have access to the NCCIC floor.

Clearly define who owns the clearance process and the steps involved to obtain it.

Streamline Portal Accesses
Accessing multiple portals (HSIN, Infraguard, DSAC, US-CERT, CISCP portals) is cumbersome and time consuming. Adopt a common portal—or use one that already exists—as the one stop, authoritative source for information sharing. One-stop shop for clearances with 1 government agency in charge and accountable, one portal that can be divided into compartments depending on which agreements you have signed and need to know. The ISACs through the National Council of ISACs have a portal in place for cross-sector sharing and this could potentially help serve as a one-stop gateway for information sharing.

Increase trust
Develop relationships and meet regularly; regular interaction leads to an increase in trust. Define information sharing guidelines. A general, lack of knowing and understanding information handling rules causes apprehension in sharing. Government and private sector must understand how each other's intelligence will be used. The FS-ISAC Traffic Light Protocol has been very effective for information sharing within the ISACs and US CERT has adopted it as well. Support and recognize originator control of information dissemination.

Improve government to government communication.
Clearly identify the roles and responsibilities for every cyber player, division, and agency from NSA to State Fusion Centers. Highlighting strengths may eliminate perceived competition between government agencies and increase trust.

Improve classified information sharing. Streamline the intelligence community tear line process and downgrading of relevant intelligence to private sector. Cleared ISAC representatives can help with this process. Educate the intelligence community on the fact that the private sector now has access to intelligence as well as its own powerful intelligence from its networks. Support recognition of the private sector as a full partner in determining what intelligence to disseminate or not disseminate, developing products and analysis.

Increase collaboration between private sector and government.
Provide threat briefings and victim notification. Bring in cleared ISAC representatives during the planning stage. Private sector liaisons can assist in providing effective content, sector perspective/reaction, etc…

Work on Joint Intelligence products. This is an exercise in joint analytics and improves the practice of information sharing. Working on Joint Intelligence products bonds intelligence

from both the private sector and government intelligence resulting in a comprehensive threat landscape.

Ensure each ISAC has a cleared representative on the NCCIC Floor. Each CIKR sector must have representation and be able to review intelligence based on their sector critical intelligence requirements.

Have various LE or CISCP analysts personally connect with partner analysts and leadership to drive participation. The idea that "welcome to the program, here's the portal, good luck!" doesn't really compel many folks to contribute.

Dedicate specific resources/analysts for the private sector support mission and empower them to share. Many USG elements have staff dedicated to relationship management (FBI KPEU for example), but we also need analysts who specifically support the private sector/critical infrastructure mission and don't have to get permission every time they talk to us and/or don't wear three hats where they support the private sector but only about 5-10% of the time.

Enable analysts to swap roles where they can sit some portion of the time with PS firms or ISACs and vice versa to generate cross-pollination of ideas and generally enhance understanding of how the sector operates. Basically, professionalize the analytic support function for Critical Infrastructure by creating a government career path, with training, and policies and methodologies for sharing that support the analysts. This is currently still an ad hoc endeavor and relies on the heroism of a few well-meaning individuals who too often have to fight their own bureaucracies to do the right thing.

Responses to Post-Hearing Questions for the Record

Submitted by Mr. David Velazquez

"Strengthening Public-Private Partnerships to Reduce Cyber Risks

to Our Nation's Critical Infrastructure"

March 26, 2014

1. *Last month the Wall Street Journal reported on a Federal Energy Regulatory Commission study that revealed grave vulnerabilities in our electric grid. The study found that the sabotage of a small, but strategic number of the tens of thousands of electrical substations across the country could cause a nationwide blackout. Do you agree with that assessment?*

No, I do not agree with that assessment. The electric grid is engineered to be resilient; this resilience includes redundancy and an ability to recover in the event critical assets are damaged or destroyed. That is not to say that a coordinated attack on several strategically chosen substations would not impact operations, but perpetrating a long-term nationwide power outage under this scenario is highly unlikely.

My understanding is that the Federal Energy Regulatory Commission (FERC) study used a static model to identify electric grid assets that are critical to the flow of electricity across the North American grid. While helpful for assessing baseline risks, static modeling does not adequately account for response. Given the ability to react to prevent a cascading outage nationwide, grid operators would seek to shed load and "island" unaffected portions of the system. If areas were affected, then the industry would move spare equipment into place or reroute power where necessary. The FERC study simply does not provide the full picture of how the thousands of owners and operators of the electric grid would work together to mitigate effects to the electric grid.

That said, static modeling is very useful for understanding which assets are critical both at the local utility level and across the North American grid. PHI analyzes its electric system and determines its electric system critical assets which includes the NERC CIP requirements. PHI has an emergency response plan to address system restoration.

Reasonable people can arrive at different conclusions about what is a truly critical asset. But with 45,000 substations in the U.S. alone, it is important that we prioritize and focus our efforts on those grid components that, if destroyed, would have the greatest impact. Static modeling helps us do that, as does the industry's partnership with law enforcement and national security experts at the federal and state level. By incorporating both government and industry perspectives, we are able to ensure the industry is focusing its efforts and resources appropriately and that priority equipment is treated as such.

2. *How vulnerable do you believe our national electric grid is to cyber attack?*

The power grid is a complex, interconnected network of generation, transmission, distribution, control, and communication technologies. Due to the interconnected nature of the nation's grid and a move toward digitization, the electric industry has seen an increasing number of threats by malicious parties to disrupt, damage and dismantle the grid either through cyber or physical attacks.

In 2013, Industrial Control System's Cyber Emergency Response Team (ICS-CERT) responded successfully to 256 incidents, 59 percent of which occurred in the energy sector, reported either directly by asset owners or through other trusted partners. ICS-CERT notes that the trusted relationship between ICS-CERT and industry, as well as an increase in awareness and reporting in the energy sector, is responsible for the increased in reported incidents.

The electric industry is forging ahead with a series of initiatives to safeguard the electric grid from threats and is partnering with federal agencies, the National Labs and 3rd party experts to improve sector-wide resilience to cyber and physical threats. The industry collaborates with the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Energy (DOE), FERC, the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and federal intelligence and law enforcement agencies to strengthen its capabilities. As threats to the grid grow and become more sophisticated, the industry remains committed to continuing to strengthen its defenses.

a. *What are your key concerns about the industrial control systems used to monitor and manage substations and equipment on the grid?*

   Electric utilities recognize that the industrial control systems used to monitor and manage substations and equipment on the grid represent the "Crown Jewels" and require significant protection measures. Although, as a general matter, electric utilities have implemented a number of procedural and technical controls to protect the industrial control systems, including among others, physical and logical separation, firewalls, intrusion detection systems, there is recognition that risk cannot be entirely eliminated and approaches to protection will need to reevaluated as cyber risk change.

   Electric utilities remain concerned about components of the supply chain particularly as it pertains to industrial control systems. This includes concerns both about the integrity of computer chips and communications modules used in industrial control systems, as well as the programming for these systems. We are pleased that recently the Department of Energy, working with energy sector owners and operators released updated procurement language[i] that will aid the sector in management of supply chain risk.

b. *How does the threat from cyber attacks compare with the physical threat to the grid?*

   Rather than attempt to compare the relative threat posed by potential cyber and physical attacks on the grid, one should consider the potential interplay between the physical and

cyber realms. It is very difficult to imagine a cyber attack with no physical implications, or a physical attack that does not also impact the cyber domain. For instance, the Metcalf Substation shooting in April 2013, that incident included a physical attack facilitated by cyber as the perpetrator cut fiber optic lines affecting 911 service in the area.

As our physical assets become increasingly reliant on cyber systems for operations and situational awareness, the industry is considering critical infrastructure protection in a more holistic way. As PHI deploys its smart grid it monitors physical intrusions as well as cyber protection in the end devices. This is consistent with PHI's all-hazards approach to threat mitigation and event response preparation.

3. *What are the cascading consequences to the national electric grid when one region loses power? What are the consequences to other critical infrastructure sectors when power is lost?*

As was observed in the August 2003 outage, uncontrolled cascading outage events in Ohio resulted in the loss of energy in parts of New York. Since then, a number of important regulatory changes have been put into place, including mandatory and enforceable standards that require utilities to follow a number of practices ranging from tree-trimming and vegetation management to cyber security measures for elements of the bulk power system.

The bulk power system in the continental United States is divided in three major sections: The Eastern Interconnect, the Western Interconnect, and the Texas Interconnection. Due to this division, electrical outages or events in the East should not impact the West or Texas. New investments also deploy advanced monitoring systems and other new technologies designed to ensure a more flexible and resilient grid such as stronger construction standards and the ability to automatically isolate and re-route around outages.

While grid operators cannot be expected to stop the threat of cyber attack, we do strive to address the vulnerabilities that threat actors seek to exploit. Grid operators are committed to security not only because of our obligation to serve consumers but also because we recognize recognition that other critical infrastructure sectors are highly dependent on reliable electricity. Water, communications, transportation, and financial services sectors may be quickly impacted if reliable electricity is not present. In addition, the Department of Defense relies heavily on electricity to accomplish their mission.

However the inter-dependencies flow both ways. While the electric grid is the only critical infrastructure segment already subject to mandatory security standards, producers of electricity require dependable water to cool theirs systems, transportation to provide fuel, communications to reliably control their equipment and financial systems to make purchases, manage credit, and pay suppliers.

[i] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM

WEDNESDAY, APRIL 2, 2014

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:12 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, presiding.

Present: Senators Carper, Coburn, McCain, and Johnson.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. The hearing will come to order.

I just want to say good morning, everyone. Thank you very much for joining us. For our first panel and for anyone on our second panel who is actually in the audience, thank you for coming, as well. To the audience, we are happy to see all of you.

I really want to extend a warm welcome to Senator Blunt, with whom I have been working on data breach issues and some others for a while. We really appreciate his participation. He is one of those people who is always interesting. He is a glass-half-full guy. He is always looking to find the middle and to figure out how we can use some common sense and collaborate.

Whenever I ask, Roy, whenever I ask people who have been married a long time, I ask them, what is the secret to being married, like, 50, 60, 70 years, and I get really hilarious answers. The best answer I ever got was two Cs, communicate and compromise. Communicate and compromise. And I would add a third C. The two Cs are also—communicate and compromise—the secret to a vibrant democracy. But if you add a third one, collaborate, I think that is the secret for us actually having some success with respect to data breach. Communicate, find principal compromises, collaborate, and the hearing today here is really designed to move us in that direction.

Senator Blunt and I have introduced a bill, the same bill, actually, for the last couple of Congresses. Is it perfect? Probably not. Could it be improved? Probably so, and what we want to do is work with the other sponsors of legislation in the Senate, and there are a number of them who have their own bills, other Committees with jurisdiction, and just work together and see if we cannot get something done, which is really what the American people sent us here to do.

There is no doubt that technology has evolved rapidly, particularly over the last decade, and these advances will continue to grow exponentially in the coming years. Technology that 10 years ago could have been something out of a science fiction movie is now a part of our daily lives. In fact, I saw a science fiction movie last night starring Woody Allen, and I am trying to remember the name of it. It came on really late at night. I turned it on as my wife was getting ready for bed and she said, "What is that?" And I said, it is a Woody Allen movie. Does anybody in the audience remember the name of it? It is just a great—pardon? "Sleeper"? Yes, I think maybe that is it. Oh, what a—— [Laughter.]

But, anyway, some of the technology in that movie, it seemed pretty outrageous then, but today, it is coming true, with a sense of humor.

But, as we embrace the latest technology both at home and in the workplace, there is little doubt that more of our sensitive personal information is at risk of being compromised. Whether it is stored in our electronic devices we use daily or on company servers, this data can be vulnerable to the threat.

As the way we communicate and do business has evolved, so have the tactics used by criminals to steal our money and steal our personal information. And today, cyber criminals run sophisticated operations and are discovering how to manipulate computer networks and make off with troves of our personal data. These data breaches have become much more prevalent, with a new one seemingly reported almost every day.

My wife now teaches at the University of Delaware and they had a breach last year. I think the State of Delaware—as an old Governor, I know the State Treasury had a breach in the last couple of years. I get these monthly reports from, I think it is Experian, telling me they are monitoring my accounts and personal data, and I was one of those people who had a credit card that we used at Target. We ultimately ended up getting a new credit card and replacing my old credit card just 3 months after I had gotten a new credit card, and I got the new credit card and it did not work. So, we know personally how it is not just inconvenience, but how this can damage our financial well-being and really cause a lot of distress.

But data breaches can put our most valuable and personal information at risk, causing worry and confusion for millions of individuals and businesses. The impact of a data breach on the average American can be extremely inconvenient and sometimes results in serious financial harm. Data breaches can also be extremely expensive for banks and other entities to respond to and remediate, including to merchants.

Although several high-profile retailers have recently come face to face with data breaches, they are not the only victims of these cyber intrusions. Hackers are targeting all types of organizations that people trust to protect their information, from popular social media platforms to major research universities, including the University of Delaware. The pervasiveness of these incidents highlights the need for us to find reasonable solutions to prevent attacks and protect consumers and businesses if a breach occurs.

We will hear in the testimony today that many retailers, financial institutions, payment processors, and the groups representing them are coming together to find common sense solutions that the private sector can undertake proactively without the help of Congress. These are groups which oftentimes find themselves on different sides of this issue.

I recognize, though, that there are many existing areas where Congress can and should play a constructive role. An important area where Congress can play a constructive role is answering the call for implementing a uniform national notification standard for when a data breach occurs. Currently, when a breach happens, notification occurs under a patchwork quilt, as we know, of 46 separate State laws. While some of these laws have common elements, creating a strong uniform national standard will allow consumers to know the rules of the road and allow business to invest the money saved from compliance into important upgrades and protections.

That is why I joined Senator Blunt to introduce our Data Security Act of 2014. We think this common sense legislation, along with other good legislation that has been introduced, as I mentioned earlier, would require a national standard for entities that collect sensitive personal information. It would require these entities to enact a cohesive plan for preventing and responding to data breaches, plans that would detail steps that will be taken to protect information, investigate breaches, and notify consumers (PIN). I will say those three things again: Protect information, investigate breaches, and notify consumers.

Most importantly, these plans would provide consistency throughout the Nation and allow consumers to have a greater level of confidence that their information will be protected and they will be notified if a breach occurs, despite whatever protective measures have been put into place. We are never going to be able to prevent every breach, I know that. We all know that. But we owe it to our consumers, we owe it to our taxpayers, we owe it to businesses and other entities that have been and will be victims of breaches to put into place the best system possible to grow with this growing threat.

We look forward to hearing from our witnesses today who are leading the voices on cybersecurity and data breach in both government and the private sector. I am sure that your insights will be valuable as we continue our efforts to fix this problem, and I am encouraged that a number of our colleagues share our interest in advancing our efforts to address data breaches.

I hope we can raise the 80/20 rule. The 80/20 rule, to our visitors here, a guy named Mike Enzi, a very good guy, a Senator from Wyoming, has this 80/20 rule. And I once asked him how he and Ted Kennedy got so much done when they took turns leading the Health, Education, Labor, and Pension Committee and he said, "Well, Ted and I subscribe to the 80/20 rule." And I said, what is that? He said, "Ted and I agree on 80 percent of the stuff. We disagree on 20 percent of the stuff. And what we do is just focus on the 80 percent where we agree and we set the 20 percent aside to another day," and I think that is what we need to do here. I hope

we will keep that in mind as we go forward, is focus on that 80 percent where we can agree.

I think it is in everyone's interest to ensure that we minimize the occurrence and impacts of data breaches, and I am sure you agree.

I am happy to turn to Dr. Coburn and then to Senator Blunt for any comments that they would like to make.

Senator COBURN. Let me defer to Senator Blunt and then I will followup.

Chairman CARPER. Senator Blunt, welcome aboard.

OPENING STATEMENT OF THE HONORABLE ROY BLUNT, U.S. SENATE

Senator BLUNT. Well, thank you.

Chairman CARPER. A former Secretary of State, I just learned today.

Senator BLUNT. as we were talking about that, both you and I, as former Statewide elected officials, have a predisposition to think that many of these things are handled better at the State and local level and that should be where we look first.

I have a prepared statement[1] I am going to leave, but I would like to say, first of all, this is an issue that has been around longer than it should have been around. You and I introduced legislation over 2 years ago, but it got a lot more attention after what happened at the end of last year and the beginning of this year.

But, I am persuaded on this topic that we cannot expect people to successfully comply with 49 different standards, and I think that is where we are now, 46 States and another three standards in Territories and other places that you have to comply with. That is an unreasonable thing to do and it is probably an impossible thing to do successfully every time you need to do it.

The other thing I would see as a hallmark of whatever we do would be that the Congress cannot be too prescriptive in how we secure this important information. I am absolutely confident that the hackers and the criminals will be more nimble than the Congress, and if you put the code in the law, you just tell them the code that has to be broken and then you have to change the law before somebody can protect themselves adequately against the code itself.

So, I would think those two things are principal goals that we should try to achieve. As Senator Carper says, there are a number of different people talking about this, and different Committees of jurisdiction. Some of you were at the Commerce Committee just the other day to talk about this same topic. But we need to move beyond talking about this to finding the solution, and I think it is really pretty simple.

If a financial institution, retailer, or a Federal agency determines that sensitive information was or may have been compromised, the bill that Senator Carper and I have proposed would simply require them to investigate the scope of the breach and determine whether the information will likely be used to cause harm or fraud, and then if the answer is yes, to notify law enforcement, to notify ap-

[1] The prepared statement of Senator Blunt appears in the Appendix on page 220.

propriate Federal agencies, consumer reporting agencies, and the consumers themselves.

There is clearly some discussion in the many discussions we have had on this about what level of breach has to be reached before you have to notify, and we are willing to have lots of input on what that number should be. I think the bill calls for one number, but that is probably not the perfect number, and frankly, whatever number we agree on probably will not be the perfect number. But, 49 different compliance regimens, an area that has driven us from one of the most secure places to do business and commerce as individuals in the world to way higher on the list of less secure than we would like to be is something that the Congress should be able to figure out a solution to.

Senator Toomey has a bill that could very well be, many elements of it, added to the bill that Senator Carper and I have proposed now for two different Congresses. I look forward to this Committee playing a real leadership role in working toward a conclusion. Surely, we have talked about this long enough and now it is time to find that solution. I am sitting here wondering if actually Senator Carper and Senator Coburn agree on 80 percent of everything, but they agree on some percent of everything and they will be the ones to figure out what percent that is, and hopefully, we can work together and get this done.

Thank you for letting me come by this morning.

Chairman CARPER. We are delighted that you are here. Thanks so much.

Dr. Coburn and I agree on about 78 percent of everything. [Laughter.]

We are closing in on 80.

Senator COBURN. Point-six-six-seven. [Laughter.]

Senator BLUNT. Point-eight percent.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Well, thank you, Senator Blunt and Senator Carper.

I would note, this is the fourth hearing on data breach in the Senate this year. And although it is an important topic, we are talking about vulnerability mitigation instead of deterrence. This Committee has had lots of testimony that we are going in the wrong direction. There is no question, I agree that we need to have some type of uniform set of standards, and I am not opposed to that. What I am opposed to is to not recognize the legitimate exposure that businesses see and why it would be in their own best interest to make sure they do not have data breaches, and I think all of them are looking at that now.

I also understand that when you spend money for vulnerability mitigation, it does not increase sales. It does not produce new products. It does not do anything to add to the bottom line. It reduces the bottom line. But, it is a necessary expenditure, just like water and heat and light and other areas.

There is no question that we have seen some serious problems in terms of data breach, but what we are not talking about today are the data breaches in the Federal Government. And to me, it is ironic that we can, as a Congress, sit and tell people, here are the

rules, and we cannot even manage our own backyard in terms of data breaches. And I will not go into it. I will put my whole statement into the record.[1]

But I think one of the important things is that we ought to be setting a good example on our own cyber within the government, and the multitude of breaches that have occurred in the Federal Government's networks would say that we are not doing that. And so we do not speak with authority on this subject until we have a track record that we, in fact, ourselves have accomplished what is necessary on our own responsibilities.

I am happy that Mr. Wilshusen is here today from the Government Accountability Office (GAO), who can really talk about what these issues are within the Federal Government and also some discussion on the EINSTEIN program, on which the Inspector General (IG) released a report just this last week. It is poorly managed and is not meeting milestones, and actually does not have the milestones and the management capabilities to get where they need to with that. Although I am a supporter of that effort, we lack that.

So, I look forward to our witnesses. I will have to leave for a period of time, but I am appreciative of the openness to talk about the whole area of data breaches, not just in the private sector. Thank you.

Chairman CARPER. Thank you, Tom.

I am going to just offer a brief introduction for each of our witnesses and then turn it over to you.

Our first witness is Edith Ramirez, Chairwoman of the Federal Trade Commission (FTC). In this capacity, she aims to prevent business practices that are anti-competitive or deceptive to consumers and enhance consumer choice and public understanding of the competitive process. Prior to joining the Commission, Ms. Ramirez was a partner in a Los Angeles law firm where she handled a broad range of complex business litigation, successfully representing clients in intellectual property, antitrust, unfair competition, and Lanham Act matters. What law firm was that?

Ms. RAMIREZ. Quinn Emanuel.

Chairman CARPER. And how long were you with them?

Ms. RAMIREZ. For 13 years.

Chairman CARPER. OK. Our second witness is William Noonan. Mr. Noonan, nice to see you. He is Deputy Special Agent in Charge of the Secret Service Criminal Investigative Division, Cyber Operations. Throughout his career at the Secret Service, he has focused on both protective and investigative missions of the agency. In his current position, he oversees the Secret Service's cyber portfolio. Mr. Noonan has over 20 years of Federal Government experience, and throughout his career, he has initiated and managed high-profile transnational fraud investigations involving network intrusions and theft of data information and intellectual property. Thank you for joining us.

Our final witness is Greg Wilshusen, Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the Federal Government and critical infrastructure. We have not seen you for almost a week, so it is nice

[1] The prepared statement of Senator Coburn appears in the Appendix on page 217.

you have come back. We are going to have to start paying you per visit. That would break the bank.

Mr. Wilshusen has over 30 years of auditing, financial management, and information systems experience and has held a variety of public and private sector positions. He is a Certified Public Accountant, Certified Internal Auditor, and a Certified Information Systems Auditor.

We thank all of you for joining us today. Your testimonies will be made part of the record. Feel free to summarize, and we will get started. I am not aware of any votes that are scheduled. Tom, are you? Ron? OK. So, I think we are good to go.

Ms. Ramirez, please proceed.

TESTIMONY OF HON. EDITH RAMIREZ,[1] CHAIRWOMAN, FEDERAL TRADE COMMISSION

Ms. RAMIREZ. Chairman Carper, Ranking Member Coburn, and Members of the Committee, thank you for the opportunity to appear before you to discuss the FTC's Data Security Enforcement Program. I am pleased to be testifying with my colleagues from the Secret Service and the Government Accountability Office.

As this Committee is well aware, consumers' data is at risk. Recent well-publicized breaches at major retailers remind us that consumer data is susceptible to compromise by those who seek to exploit security vulnerabilities. This takes place against the background of the threat of identity theft, which has been the FTC's top consumer complaint for the last 14 years.

The Commission is here today to reiterate its bipartisan and unanimous call for Federal data security legislation. Never has the need for such legislation been greater. With reports of data breaches on the rise, Congress needs to act, and I would like to thank you, Chairman Carper, for your longstanding attention to the issue of data security.

The FTC supports Federal legislation that would strengthen existing data security tools and require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Reasonable security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. And, when breaches do occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data.

Legislation should give the FTC authority to seek civil penalties where warranted to help ensure that FTC actions have an appropriate deterrent effect. In addition, enabling the FTC to bring cases against nonprofits, such as universities and health systems, which have reported a substantial number of breaches, would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

Finally, Administrative Procedure Act (APA) rulemaking authority, like that used in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN–SPAM), would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, com-

[1] The prepared statement of Ms. Ramirez appears in the Appendix on page 227.

panies would be required to give adequate protection to such data. For example, whereas a decade ago, it would have been difficult and expensive for a company to track an individual's precise location, smartphones have made this information readily available. And in recent years, the growing problem of child identity theft has brought to light that Social Security numbers alone can be combined with another person's information to steal an identity.

Using its existing authority, the FTC has settled 52 civil actions against companies that we alleged put consumer data at risk. In all these cases, the touchstone of the Commission's approach has been reasonableness. A company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.

The Commission has made clear that it does not require perfect security, and the fact that a breach occurred does not mean that a company has violated the law.

A number of the breaches that have prompted FTC civil enforcement action have also led to investigation and enforcement by criminal authorities. For example, in 2008, the FTC settled allegations that security deficiencies of retailer TJX permitted hackers to obtain information about tens of millions of credit and debit cards. At the same time, the Department of Justice (DOJ) successfully prosecuted a hacker behind the TJX and other breaches.

As the TJX case illustrates, the FTC and criminal authorities share complementary goals. FTC actions help ensure, on the front end, that businesses do not put their consumers' data at unnecessary risk, while criminal enforcers help ensure that cyber criminals are caught and punished. This dual approach to data security leverages government resources and best serves the interests of consumers, and to that end, the FTC, the Justice Department, and the Secret Service have worked to coordinate our respective data security investigations.

The TJX case is also a good illustration of the Commission's approach to data security enforcement. In our case against TJX, the FTC alleged a failure to implement basic, fundamental safeguards with respect to consumer data. More specifically, the Commission alleged that the company engaged in a number of practices that, taken together, were unreasonable, such as allowing network administrators to use weak passwords, failing to limit wireless access to in-store networks, not using firewalls to isolate computers processing cardholder data from the Internet, and not having procedures to detect and prevent unauthorized access to its networks.

In addition to the Commission's enforcement work, the FTC offers guidance to consumers and businesses. For those consumers affected by recent breaches, the FTC has posted information online about steps they should take to protect themselves. These materials are in addition to the large stable of other FTC resources we have for ID theft victims. We also engage in extensive policy initiatives on privacy and data security issues.

In closing, I want to thank the Committee for holding this hearing and for the opportunity to provide the Commission's views. Data security is among the Commission's highest priorities, and we

look forward to working with Congress on this critical issue. Thank you.

Chairman CARPER. Ms. Ramirez, thank you so much for that testimony.

Mr. Noonan, welcome. Please proceed.

TESTIMONY OF WILLIAM NOONAN,[1] DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, CYBER OPERATIONS BRANCH, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. NOONAN. Thank you, sir. Good morning, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Homeland Security (DHS) regarding the ongoing trend of criminals exploiting cyberspace to obtain sensitive financial and identity information as part of a complex criminal scheme to defraud our Nation's payment systems.

Our modern financial system depends heavily on information technology (IT) for convenience and efficiency. Accordingly, criminals, motivated by greed, have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment systems to engage in fraud and other illicit activities. The widely reported payment card data breaches of Target, Neiman Marcus, White Lodging, and other retailers are just recent examples of this trend. The Secret Service is investigating these recent data breaches and we are confident we will bring the criminals responsible to justice.

This year is the 30th anniversary of when Congress first defined as specific Federal crimes both unauthorized access to computers and access device fraud, while explicitly assigning the Secret Service authority to investigate these crimes. Over the past three decades, the Secret Service has continuously innovated in how we investigate these crimes and defeat the criminal organizations responsible for major data breaches.

In support of the Department of Homeland Security's missions to safeguard cyberspace, the Secret Service has developed a unique record of successes investigating cyber crime through the efforts of our highly trained special agents and the work of our growing network of 35 Electronic Crimes Task Forces, which Congress in 2001 assigned the mission of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

As a result of our cyber crime investigations, over the past 4 years, the Secret Service has arrested nearly 5,000 cyber criminals. In total, these criminals were responsible for over a billion dollars in fraud losses, and we estimate investigations prevented over $11 billion in fraud losses.

Data breaches like the recently reported occurrences are just one part of the complex criminal scheme executed by organized cyber crime. These criminal groups are using increasingly sophisticated technology to conduct a criminal conspiracy consisting of five parts.

[1] The prepared statement of Mr. Noonan appears in the Appendix on page 239.

One, gaining unauthorized access to computer systems carrying valuable protected information.

Two, deploying specialized malware to capture and exfiltrate this data.

Three, distributing or selling this sensitive data to their criminal associates.

Four, engaging in sophisticated distributed frauds using the sensitive information obtained.

And, five, laundering the proceeds of this illicit activity.

All five of these activities are criminal violations in and of themselves, and when conducted by sophisticated transnational networks of cyber criminals, this scheme has yielded hundreds of millions of dollars in illicit proceeds.

The Secret Service is committed to protecting our Nation from this threat. We disrupt every step of their five-part criminal scheme through proactive criminal investigations and defeat these transnational cyber criminals through coordinated arrests and seizure of assets.

Foundational to these efforts are our private industry partners as well as the close partnerships that we have with the State, local, Federal, and international law enforcement. As a result of these partnerships, we are able to prevent many cyber crimes by sharing criminal intelligence regarding the plans of cyber criminals and by working with victim companies and financial institutions to minimize financial losses.

Through our Department's National Cybersecurity and Communications Integration Center (NCCIC), the Secret Service also quickly shares technical cybersecurity information while protecting civil rights and civil liberties in order to enable other organizations to reduce their cyber risks by mitigating technical vulnerabilities.

We also partner with the private sector and academia to research cyber threats and publish the information on cyber crime trends through reports like the Carnegie Mellon CERT Insider Threat Study, the Verizon Data Breach Investigations Report, and the Trustwave Global Security Report.

The Secret Service has a long history of protecting our Nation's financial system from threats. In 1865, the threat we were founded to address was that of counterfeit currency. As our financial payment system has evolved, from paper to plastic to now digital information, so, too, has our investigative mission. The Secret Service is committed to continuing to protect our Nation's financial system, even as criminals increasingly exploit it through cyberspace.

Through the dedicated efforts of our special agents, our Electronic Crimes Task Forces, and by working in close partnership with the Department of Justice, in particular, the Computer Crimes, Intellectual Property Section, and local U.S. Attorney's Offices, the Secret Service will continue to bring cyber criminals that perpetrate major data breaches to justice.

Thank you for the opportunity to testify on this important topic, and we look forward to your questions.

Chairman CARPER. Thank you so much. I enjoyed meeting with you last week and learned a lot from that conversation, and I am sure we will learn a lot more here today. Thanks.

Mr. Wilshusen, welcome aboard.

TESTIMONY OF GREGORY C. WILSHUSEN,[1] DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Thank you. Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee, thank you for the opportunity to testify at today's hearing on data breaches. My testimony today will address Federal efforts to protect its information and to respond to data breaches that occur.

Before I begin, if I may, I would like to recognize several members of my team, including John de Ferrari and Jeff Knott, who are sitting behind me, and Larry Crosland and Marisol Cruz, who conducted the work underpinning my testimony today.

Chairman CARPER. Would they raise their hands, please? Thank you.

Mr. WILSHUSEN. In addition, Lee McCracken was instrumental in crafting my written statement.

Mr. Chairman, as you know, the Federal Government collects and retains large volumes of sensitive information, including personal information on American citizens. The loss or unauthorized disclosure or alteration of this information can lead to serious consequences and substantial harm to individuals, as well as the Nation.

Over the past 4 years, the number of information security incidents reported by Federal agencies involving personal information has more than doubled, to 25,566 in fiscal year (FY) 2013.

Agencies continue to face challenges in securing their information. They have had mixed results in addressing the eight components of an agency-wide information security program called for by law, and most of the 24 agencies covered by the Chief Financial Officers Act have had weaknesses in implementing key security controls.

In fiscal year 2013, for example, 18 of the 24 agencies reported a significant deficiency or material weakness in information security controls for financial reporting purposes. IGs at 21 agencies cited information security as a major management challenge for their agency. And GAO once again designated Federal information security as a Governmentwide High-Risk Area.

Mr. Chairman, even when agencies have implemented effective information security programs, data breaches can still occur, so it is imperative that agencies respond appropriately. At the request of this Committee, we issued a report in December on agency responses to breaches of personally identifiable information (PII). We determined that agencies included in our review had generally developed policies and procedures for responding to data breaches and had implemented key preparatory practices that should be performed in advance of specific incidents, and these include establishing a Data Breach Response Team to oversee response activities and training employees on the roles and responsibility for breach response.

However, agencies' implementation of key operational practices that should be performed in response to specific incidents was inconsistent. Although all the agencies reviewed had prepared and

[1] The prepared statement of Mr. Wilshusen appears in the Appendix on page 250.

submitted reports of incidents to appropriate authorities, they did not consistently implement other key response practices.

For example, of the seven agencies we reviewed, only the Internal Revenue Service (IRS) consistently assigned a risk level for each data breach reviewed and documented how that level was determined.

The seven agencies documented the number of individuals affected by a breach in only 46 percent of the 363 incidents we reviewed. And only the Army and Securities and Exchange Commission (SEC) notified all affected individuals for each breach determined to be high-risk. In total, individuals were not notified in about 22 percent of the high-risk incidents.

The seven agencies also did not consistently offer credit monitoring to individuals affected by PII-related breaches, and none of the agencies consistently document lessons learned from data breaches, including corrective actions to prevent or detect similar incidents in the future.

We also reported that the Office of Management and Budget (OMB) requirement for agencies to individually report each PII-related incident involving paper-based information or the loss of hardware with encrypted data to U.S. Computer Emergency Readiness Team (US–CERT) within 1 hour of discovery added little value beyond what could be achieved by periodic consolidated reporting. We recommended that OMB revise its reporting requirements and update its guidance to improve the consistency and effectiveness of agency data breach response programs. We also made 22 recommendations to agencies to improve their data breach response practices.

At the request of this Committee, we also studied Federal agencies' ability to respond to cyber incidents. We determined the extent to which Federal agencies are effectively responding to cyber incidents once they have been detected and the extent to which DHS is providing assistance to agencies. We plan to issue our report later this spring.

Chairman Carper, Dr. Coburn, and Members of the Committee, this concludes my statement. I would be happy to answer any questions.

Chairman CARPER. Greg, thanks so much for joining us again this week.

You have mentioned and Dr. Coburn has mentioned the ability of the Federal Government to protect its own sensitive information. There is an old law called the Federal Information and Security Management Act which needs desperately to be updated. One of the things—Dr. Coburn is threatening to leave us at the end of this year, as you may know, and one of the things I am very hopeful that we will be able to do is update that legislation. We are working on it, our staffs are working on it, and we appreciate very much your help in doing that.

I think it was Abraham Lincoln who once said the role of government is to do for the people what they cannot do for themselves. With that thought in mind, what I really hope we can accomplish here today—I do not want to have a hearing just to have another hearing on data breach. We have all these different ideas, legislation from good people, Democrats, Republicans, and we have to get

on the same page. We have to stop talking past each other. And, I think as the retailers, as the card issuers, as the card processors are coming together, creating their own coalition to look for ways to collaborate, that, I think, helps us to better figure out what we need to do and to guide us.

But, here is what I am going to ask this panel, each of you, and I am going to ask the second panel, as well, is what does the Congress need to do? And to the extent that we can find some concurrence on that question, that would be hugely helpful. What do we need to do? Let me just start off with Chairwoman Ramirez, please. What does the Congress need to do? And maybe the second half of my question is, what do we need not to do?

Ms. RAMIREZ. Let me focus on the first question that you posed, which I think is the central question to ask today. From our perspective at the Federal Trade Commission, we think that it is absolutely time for Congress to enact comprehensive Federal legislation in this area, setting robust standards and data breach notification requirements. And specifically, what we ask is that this legislation provide civil penalty authority to the FTC to augment our existing work in this arena and to ensure that there is appropriate deterrence and that companies invest appropriately and institute reasonable security measures to protect consumer information.

We also think it is important for any legislation to give the FTC APA rulemaking authority, which——

Chairman CARPER. I am sorry. APA——

Ms. RAMIREZ. Administrative Procedure Act. This would enable us to make rules to implement any legislation, and the reason that we think it is so necessary to have this authority is that it is really critical that we be provided the tools so that any legislation can be adapted to changing and evolving technology. And I mentioned in my opening statement today, geolocation information is readily available. A decade ago, that certainly was not the case, and we need to be able to adapt to changing times, both to be able to, if necessary, redefine what constitutes personal information, but then also, perhaps, to lift any requirements that may no longer be necessary, given the evolution of technology.

And then, finally, we also ask that we be provided jurisdiction over nonprofits, which we currently lack. Today, we also know that university systems and nonprofit hospitals that are currently outside of our jurisdiction also have suffered breaches and we think it is important that the FTC have authority in this area.

Chairman CARPER. OK. Thanks.

Mr. Noonan, if you and Mr. Wilshusen—feel free to react to what Ms. Ramirez has said, points that you agree with, maybe those that you do not. But again, the idea is for us to better understand today what the Congress needs to do and what we do not need to do and looking for consensus here. If we can find some of that, that would be great.

Mr. NOONAN. I think, generally, the consensus that I have is that we do need to establish a national bill where disclosure is made. Important to the Secret Service, and, I think, to the country, is there should be a piece there where there is notification or disclosure of data breaches to law enforcement with jurisdiction. Law enforcement plays a critical role in data breach investigations, both

in law enforcement going after the criminal piece as a deterrent, but also as an information sharing piece, what we learn out of these data breaches and then how we are able to take that information and share it back with critical infrastructure.

So, I think that is a critical piece of any national legislation that should potentially go forward, as well as increasing the penalties for these types of activities. If Congress were to increase the penalties of 18 USC 1030, potentially, that would act as a deterrent for criminals from coming into protected computer systems, as well as having 1030 act as a predicate offense to Racketeering and Organized Crime standards, so we can get higher-level prosecution.

So, in our exposure and in what we have learned, too, is that the higher the level of penalties, the higher the level of cooperation sometimes is amongst some of the people that we bring to justice, and they are able to share information back with the government so we can prevent further acts from occurring.

Chairman CARPER. OK. Mr. Wilshusen, same question, please.

Mr. WILSHUSEN. I would say one thing that Congress can do is to look at the Federal Information Security Management Act (FISMA) reform within the Federal space. As you know, FISMA gives OMB several responsibilities for overseeing and assisting agencies in their implementation of information security controls. OMB has delegated or transferred many of those responsibilities to the Department of Homeland Security, and so clarifying the roles and responsibilities of those two organizations for overseeing information security within the Federal space could be very helpful.

I also think, that this Committee and others should continue to provide the oversight necessary within the Federal space and to assure that proper attention is given to protecting information security, not only within the Federal Government, but also in its interactions with critical infrastructure protection and other roles in helping our citizens protect information that they also have out on the Web and Internet.

One thing Congress should not do is to turn a blind eye. Keep attention focused on this area.

Chairman CARPER. OK. Thanks very much.

Senator McCain, welcome.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Well, thank you, Mr. Chairman.

Ms. Ramirez, so that people and perhaps Members of Congress can understand better what is going on here, let us talk a little bit about the data breach at Target Corporation. Apparently, there was some Russian input into it, or there may have been that there was Russian language or something like that into what we were able to ascertain about these hackers, is that right?

Ms. RAMIREZ. Senator, let me just emphasize, the FTC focuses on the civil law side of this, and on the front end. And this is an investigation that Target has confirmed that the FTC is looking at it. I cannot comment on any pending investigation——

Senator MCCAIN. Mr. Noonan, can you comment? It is in the public record, I mean. It is not a secret. Is there——

Chairman CARPER. Can I just interject something, John? Mr. Noonan came and met with us in my office last week. He gave a

great explanation of what happened at Target that even I could understand, and——

Senator MCCAIN. Go ahead. And I am also interested in the financial loss there so that people can understand better the magnitude of this breach, which is symptomatic of many others. Go ahead, Mr. Noonan.

Mr. NOONAN. Sure, sir. I just want to kind of crosswalk you across these data breaches, these major data breaches, exactly how these intrusions occur and the nationality that we are talking about. These are transnational organized criminals. To say that it is one country that these people are from, it would be inaccurate if I told you that. I would like to say that——

Senator MCCAIN. But there are some allegations that some of this has come from Russian sources.

Mr. NOONAN. So, a majority of these people that are attacking these systems are from Eastern Europe. They use the Russian language as a means to be able to communicate in——

Senator MCCAIN. I got you.

Mr. NOONAN [continuing]. As an operations security (OPSEC), if you will, to keep domestic law enforcement out of their wares.

So, the way it works it is not one criminal, it is not one criminal group, it is a loosely affiliated group. So, there are people out there that are gaining access to computer systems and they are potentially selling access on criminal undergrounds to one another.

There are other people that are developing malware and that malware is then used by another person or another group that may insert that malware into the compromised system.

There are other pieces of the organization that will test that malware to make sure that that malware is not susceptible to our antivirus means that are out there to stop this.

You have to understand, these people are motivated by greed. So, when they go into a system, they have to be quiet. They cannot be found or discovered. Otherwise, they are not going to achieve their goal, and that is to exfiltrate out the data which they can sell. Exfiltrate, in the cases of a lot of the data breaches that are in the media right now, are related to payment cards, but that is just not what they are after. They are after whatever it is that they can monetize. So, I think that we have brought up the fact that personally identifiable information, is a piece that can be monetized and such.

So, in the underground, once that data is exfiltrated out, there is a criminal underground that works on vending that data. So, they sell to other criminals across the world who then use that for their personal gain.

And then there is a money laundering system where the money flow goes back, and when we talk about money flow, we are not talking about currencies. We are talking about digital currencies on how the money is moved back, where it is not traceable. It is very difficult for law enforcement to trace the movement of that money where it is not regulated.

So, that is the type of criminal organizations we are talking about——

Senator MCCAIN. So, in the case of Target, how much money are we talking about?

Mr. NOONAN. We are not at the point in our investigation where we can lock down a dollar amount, but we believe it is probably going to be several million dollars were at risk.

Senator MCCAIN. And no matter who is responsible, eventually, that cost is passed on to the consumer, and Target is just one of many, perhaps one of the more visible, but Neiman Marcus and others, this has happened. And there is no reason to believe this is going to stop, would you agree?

Mr. NOONAN. I believe that with the assistance of law enforcement, we are moving toward getting certain individuals to be able to stop this action as a deterrent. I would hope that we would be able to bring these criminals to justice. So, I think it is a long string, a long history of attacks that have occurred, and I think what our—and to your point, wherever we raise the fence, I think these criminals, because of their motivation, will always be looking for the edge of the fence. So, there is no silver bullet that is going to be able to take care of the problem.

Senator MCCAIN. And you would, as you have already stated, Ms. Ramirez, that different State laws obviously does not get it, that there needs to be Federal legislation.

Ms. RAMIREZ. State laws only address the breach notification aspect of this, so I think there does need to be a Federal standard. And based on our own experience and what we look at, which is the measures that companies have in place, it is clear that companies are not investing adequately in the area of data security and that more needs to be done.

Senator MCCAIN. Mr. Wilshusen, you stated in your testimony that in a 2013 GAO report, GAO made 22 recommendations to Federal agencies which aim to improve data breach response activities. How are these agencies responding to those recommendations?

Mr. WILSHUSEN. Well, we made recommendations to nine agencies. Four of them agreed and concurred with all the recommendations that we made. Three neither concurred or non-concurred. And we had two that agreed with one of our recommendations each to them, but disagreed, non-concurred, with the other recommendations we made to them.

Senator MCCAIN. Mr. Chairman, we ought to find out the reason why several of these agencies did not concur. They may have had some reason that I cannot detect, but this GAO report, I think, were common sense addressing some of these issues.

So, you have not seen the kind of compliance or implementation of your recommendations that you think are adequate?

Mr. WILSHUSEN. We just made the recommendations back in December. In the responses, six of the agencies indicated some of the actions that they were taking to implement our recommendations, and we will followup over the course of the year, and we will do so annually, to assess the status of their corrective actions in implementing our recommendations.

Senator MCCAIN. When do we expect to hear from you next?

Mr. WILSHUSEN. Whenever you invite me.

Senator MCCAIN. I mean, as far as the assessment is concerned.

Mr. WILSHUSEN. That would be later this year.

Senator MCCAIN. Like——

Mr. WILSHUSEN. Toward the end of the year, when we will check to see if—the first time we will hear something back from them will be in their 60-day letter to us on the status of their actions and final determinations of concurrence with our recommendations.

Senator MCCAIN. Thank you, Mr. Chairman.

Chairman CARPER. Dr. Coburn.

Senator COBURN. Chairwoman Ramirez, in your oral testimony, you talked about civil penalties creating the deterrence effect. You were talking about a deterrence for businesses to be compliant with what they need to be. The deterrence I am talking about is what Mr. Noonan—so, of the 52 cases that you had authority in, and one of your statements is that you needed greater authority to hold them. Of those 52 cases, in how many were the perpetrators prosecuted?

Ms. RAMIREZ. Senator, I am going to need to get back to you with a particular figure, but what I can tell you is that we work very closely with the criminal authorities. We coordinate with Mr. Noonan and his team on a number of different matters. So, even though we focus on what we call the front end, the way businesses are implementing data security measures, we do, of course, understand it is absolutely critical that criminal law enforcers go after——

Senator COBURN. Well, that is the real answer, because as soon as—here is the problem. When it is all regulatory authority to make compliance versus punishing the people who are violating the compliance, in other words, the people who are probing the networks, we are never going to get ahead of this. And we have had very strong testimony before this Committee that if you focus on mitigation vulnerabilities, mitigating the vulnerabilities in your network, and you do not put 60 to 70 percent of your time in terms of prosecuting the mal-actors, we are never going to win this battle. We can have the strongest networks in the world and there is always going to be somebody who goes after it.

So, if we create the expectation in this country that if you are violating a network, you are going to get hammered, what we are going to do is markedly increase not only the events that happen, but the costs associated with protecting networks. And so I think it is really important that we look at that, and it bothers me a little bit, even though you say you work with them, the point is, you need to have a balanced approach. It needs to be both. It cannot just be businesses comply with this regulatory regime and you are fine, because we will never stop it.

Ms. RAMIREZ. Senator, if I may, just so that I can clarify this point, my view is that this is a very complex problem that requires multiple prongs. At the FTC, we only have certain authority. We have civil law authority and our authority goes to the businesses that put data security measures in place. We think there is underinvestment in that arena and that needs to be addressed. But, absolutely, all the points that you raise are absolutely valid, and we do collaborate with the other agencies that have another part to play in this arena.

Senator COBURN. One other question. Of the 52 cases where you had the authority to work, how many other cases have you had greater authority? Where were you limited by not having additional

authority? Can you name examples of places where you saw a problem but you did not see the authority to get the problem corrected?

Ms. RAMIREZ. Well, the additional authority that we seek is very targeted. So we are asking for civil penalty authority, because today, we do not have, under our Section 5 authority, we do not have the ability to impose penalties, and we do think that it is necessary to have greater deterrence in this arena. We are also asking for——

Senator COBURN. Well, you really mean compliance. You do not mean deterrence. Deterrence is going after the bad actors. Compliance is what you really——

Ms. RAMIREZ. Well, we——

Senator COBURN. Is that right?

Ms. RAMIREZ. No. We view deterrence also in terms of companies providing reasonable security measures and providing adequate protection to consumers.

Senator COBURN. OK. Mr. Noonan, I am proud of the work that you all do and appreciate all of you being here. One of the other things that we had in our testimony was that we have very few Federal Bureau of Investigation (FBI) agents with which you can work that cooperate overseas on investigating. Do you see that as a problem as you all work these cases?

Mr. NOONAN. To have the number of agents that are overseas in our overseas offices?

Senator COBURN. Well, not just your agents, but also FBI agents. Do you not work in conjunction with FBI on a lot of this stuff?

Mr. NOONAN. Yes, sir. So, we do coordinate with the FBI on a lot of these cases.

Senator COBURN. But the testimony was there is really a slim number of those people with which to work. Do you see that as a problem as you try to execute prosecution and investigation on these cases? Do you see a lack of resources, as far as coming from the FBI, coordinating with you, with our partners overseas as we try to prosecute these events?

Mr. NOONAN. What I see is that we, together, have a unique history of bringing cyber criminals to justice. What I do think is that our relationship building is probably the most critical piece that we in Federal law enforcement have overseas. We do not have jurisdiction to really work in these overseas environments, but I think in Federal law enforcement, it is based on the relationship building and our efforts of coordinating with Federal—with other international law enforcement.

So, as far as the numbers of people, could we always have more to assist in building that liaison and building on that coordination? Absolutely. But, I think it is based on our efforts, the Secret Service efforts, in our international offices and our working groups in developing those relationships with those international partners that is aiding us in bringing those different criminal actors in Eastern Europe to justice here domestically. We have a great——

Senator COBURN. I understand that, but here is what I am trying to get at. Mr. Chabinsky testified last week, Steve Chabinsky, that we have few FBI agents working overseas to try to coordinate to help you do that. And my question is, do you see that as a problem or not a problem? Do you dispute his testimony?

Mr. NOONAN. No, I would not dispute the Director's testimony.

Senator COBURN. So, we do need more resources on the FBI to coordinate with you, with our partners overseas?

Mr. NOONAN. I think with all of Federal law enforcement, we would—and not just necessarily the FBI, but also with the Secret Service in our international capacities over in the international footprint, as well.

Senator COBURN. OK. Mr. Wilshusen, would you clarify. Twenty-five-thousand-five-hundred-and-sixty-six events in 2013. Describe what you mean by "event."

Mr. WILSHUSEN. OK. Those would be incidents reported by Federal agencies to the US–CERT, and those can include various different types of security incidents. These all involved personal information or personally identifiable information, as opposed to other incidents which do not. And——

Senator COBURN. So, all 25,000 of these were PIIs?

Mr. WILSHUSEN. Yes, that is correct——

Senator COBURN. OK.

Mr. WILSHUSEN [continuing]. As reported by Federal agencies to the US–CERT. About 25 percent of all incidents including non-PII incidents were non-cyber incidents. Another 16 percent of those could be due to equipment loss or theft of equipment which contained PII data. Some of that data may have been encrypted on those machines, some perhaps not. And others included the implementation of—or installation, excuse me, of malicious code onto devices and onto the systems. It could also include, for example, policy violations, where individuals may have violated their agency's policy related to protecting or using personal information.

Senator COBURN. OK. The other part of your report is that operational practices were inconsistent pretty well throughout the government.

Mr. WILSHUSEN. Throughout the seven agencies that we reviewed as part of that review, and those agencies included the Army, Centers for Medicare and Medicaid Service (CMS), IRS, Department of Veterans Affairs, Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board, Securities and Exchange Commission, and the Federal Retirement Thrift Investment Board.

Senator COBURN. OK. Chairman Carper and I, as well as the Commerce Committee and the Intelligence Committee, have the job of putting together a cyber bill this year. Hopefully, we will get that done. Any comments from any of you all on things that we should look at that will make your job easier and at the same time make us more effective as a Nation in terms of cybersecurity?

Mr. NOONAN. Yes, sir. In fact, we spoke earlier in the week about an issue regarding notification. We believe it is important to allow law enforcement to have an active role in these types of investigations.

The late notification is a piece that we talked about as it relates to notification out to victims. So, when we potentially identify a victim company, the victim company, of course, has an obligation where they would like to inform its victims of the exposure, if you will.

There are many times where law enforcement has ongoing operations, whether they are undercover operations or working with

sources, which have the ability to get at the potential root that we talked about in a deterrent factor to try to gather more evidence and to identify who the criminal actors potentially are. So, in a case where law enforcement would work with the victim company and allow them to have a delay in their notification out to the individual victims——

Senator COBURN. It would give us an advantage to travel back.

Mr. NOONAN. Potentially, yes, sir.

Senator COBURN. OK.

Mr. NOONAN. So, I think it is very important—in fact, I can crosswalk you through a case that we not too recently, but we have recently had, where we were engaged in an undercover operation where we had the opportunity to not only advise that company of their data breach, but after we had advised them of their data breach, we entered into an operation where we could actually obtain that data and get that data. The company was very quick and wanted to notify its consumers to the point where it was interfering with the operation. So, that is what——

Senator COBURN. So, we need to have the flexibility in any data act or cyber bill we have to protect the law enforcement to be able to do their job and continue a sting or something similar to that. In other words, there needs to be a variance if and when law enforcement says, please wait one week until we finish what we are doing.

Mr. NOONAN. Yes, sir. So, the word I would use is a compromise. So, there must be a compromise. When I use the word "compromise," I mean notification should not be delayed by months and years. It should be a reasonable amount of time.

Senator COBURN. All right. Anybody else?

Mr. WILSHUSEN. I would just add, as it relates to FISMA and within the Federal space, just to clarify the roles and responsibilities of the Office of Management and Budget and the Department of Homeland Security with overseeing and assisting Federal agencies in implementing information security.

Senator COBURN. Well, the only way you are going to get it implemented is have some teeth in it, and the only organization that has teeth right now is OMB. Homeland Security is coming on strong. They are improving rapidly, thanks to Senator Carper and the new Secretary and some of the work that was done before they got there. But it is important that we get a bill that causes people to buy into what we need to do on a timely basis.

Thank you, Mr. Chairman.

Chairman CARPER. You bet.

I want to go back to the questioning that was going on with Dr. Coburn and really with you, Mr. Noonan, on notification. I think I said earlier in my comments, I said there are three things we are focused on here. One, how do we protect information? Two, how do we investigate when there are problems? And, three, how do you go about notification? Another one would probably be, do we continue to have 40-some standards or do we compress that to one national standard, or something in between 49 and one that we should do.

But, let us just stick with notification for a little bit. I heard from some sources that if people get notified too often, consumers get no-

tified repeatedly for even minor breaches, that they come to a point where they become almost numb to the notifications. Can any of you comment on that, trying to figure out when should the notification occur for an individual to avoid that, if that is a legitimate concern?

Ms. RAMIREZ. Chairman, I am happy to answer your question. I think it is a balance. We at the FTC are certainly very sensitive to the concern that you raise about potential over-notification. What we think needs to be done is that consumers need to be notified if there is a reasonable risk of harm. So, the——

Chairman CARPER. How do we go about——

Ms. RAMIREZ. Well, it is a fact-specific test, but I think it is important that a company that holds consumer data have an opportunity before there is any notification to assess and determine exactly what data might have been compromised, and then based on that information, and based on the sensitivity of the information, that, in turn, can be used to determine when and who ought to be notified. So, I do think it is a balance, but I think the test ought to be a reasonableness test, and if there is a reasonable risk of harm to consumers, there ought to be notification.

Chairman CARPER. OK. Others, please.

Mr. WILSHUSEN. Yes.

Chairman CARPER. Mr. Wilshusen.

Mr. WILSHUSEN. Yes. Within the Federal space, agencies are supposed to assess the risk and level of impact that could occur once a data breach occurs; that is the level of harm that could occur to the affected individual. There are a number of factors that they take into account, or should take into account to determine that level of risk.

Those include one the type of information that was actually compromised, whether it is just a name or is it the name and Social Security number and other personal information, and the two nature of the breach. Is it one in the case of where, for example, the PII is on a laptop for which the data is encrypted? The risk would be lower than if someone had intruded on a network and was exfiltrating this information out of the network.

And so taking those factors and considering the risk of harm that could occur with the information that was compromised would be another factor in determining the level of risk, and also just the number of people that may be impacted by that incident.

And based on that, make a determination on whether notification should be made to the affected individual, because as you point out, you do not want to unnecessarily or unduly notify someone who will really have a very minor or limited risk of their information being compromised. But if that risk is reasonable or high, certainly, notification should probably be made.

Chairman CARPER. Mr. Noonan, anything else you want to mention on this?

Mr. NOONAN. Yes, sir. I think it is also important to give a company the opportunity to look at its own systems. So, a lot of times, you are going to understand, in the report that we have worked with—the Verizon data breach, on the Verizon Data Breach Report, just last year, together, Verizon reported that over 70 percent of the disclosures to a victim company were made by an outside

source, so, by law enforcement or another to the victim company saying that they have a problem. So, when that occurs, the company needs to take a look at itself within and determine if and when it actually did have a compromise and an exfiltration of that data.

That being said, companies do need to have a window of time to be able to do an internal investigation to determine if there is actually a problem from the notification from law enforcement. So, it is not an instant occurrence where law enforcement comes to them and says, we believe you have a problem. They still have to take an opportunity to work with third-party forensic companies to take a look at their systems to determine if they do have a problem. So, by requiring too quick of a notification, it could damage the company or the company's reputation, as well. So, we think that is an important part, to give leverage to companies.

Chairman CARPER. OK. Good. One last question, and then we will excuse this panel and invite our second panel to join us. But in our next panel, we are going to hear from Governor Pawlenty, representing the Financial Services Roundtable, Ms. Kennedy from the Retail Industry Leaders Association about common sense solutions that the private sector can undertake proactively without the help of Congress. And these are groups which oftentimes find themselves, as you know, on different sides of an issue, and certainly this issue, so it is actually quite encouraging that they are taking steps to work together to get their arms around this very difficult issue.

Can each of you just offer some advice to the new Working Group that has been formed in recent weeks. Just give them some advice, if you will. And, also, what should they be focusing on? What should they be focusing on? Who should they be talking to in order to make sure they are getting all the information that they need?

Mr. NOONAN. Yes, sir. So, the Secret Service and law enforcement work together collaboratively, especially since Secret Service has been so engaged in the area and the lane of the financial services sector. We work very closely with the Financial Services Information Sharing and Analysis Centers (FS–ISAC).

We have developed a very close relationship, not just at their headquarters level, but throughout the country in our field offices. So, we have a group of 35 Electronic Crimes Task Forces throughout the country that those task forces have active members of the FS–ISAC sitting with them in these task force environments sharing information back and forth. Not to mention that the ability of the FS–ISAC, the Information Sharing and Analysis Center for the Financial Services Sector, they also sit up at the NCCIC. They sit on the NCCIC floor, where information flows freely and the FS–ISAC is able to take that information that they learned on the NCCIC floor and share that out with its different members.

So, again, any new Information Sharing and Analysis Center, should do a couple of different things. It should develop a robust relationship with the Department of Homeland Security and the NCCIC and try to secure a position on that floor so they can gain access to that valuable information to share with its members, as well as develop a relationship with the law enforcement, Federal law enforcement. We believe that relationship is done through the

network of our 35 Electronic Crimes Task Forces, which its members can join through any one of those task forces or through one of the local Secret Service offices.

Chairman CARPER. OK. Thank you.

Just briefly, Mr. Wilshusen, please.

Mr. WILSHUSEN. OK. I would just piggyback on what Mr. Noonan mentioned, and that is, and as we testified at last week's hearing, is to remove the barriers that would allow for effective information sharing of these threats, alerts, as well as other incidents that occur in this space.

Chairman CARPER. Good. Thanks.

Ms. Ramirez, just very briefly, please.

Ms. RAMIREZ. Let me just say that I applaud all of these efforts. From our perspective, anything that could be done to increase protection for consumer information is a good step.

Chairman CARPER. OK. Good.

We are going to excuse you now, but we want to continue this conversation and we very much appreciate your input. You are part of the solution and we are, too, and we need your help and we appreciate the kindness and the counsel you have given us today. And we are determined to communicate, to find principal compromises, and to collaborate, and we look forward to doing all those things with you. Thank you so much.

With that, we are going to have a brief recess while the next panel comes forward. Again, it is great to see you all. Thanks so much for your help.

[Recess.]

Hello. From one recovering Governor to another, welcome aboard.

Ms. Kennedy, nice to see you again.

Tiffany Jones, thank you so much for coming.

You heard a little bit of advice there from the first panel to each of you and I hope you will take it to heart. We will, as well.

But, our first witness is the Honorable Tim Pawlenty. Governor Pawlenty he used to be Chief Executive Officer for his State, and I still say that is the best job around, at least for a guy in our business—but, Chief Executive Officer now for the Financial Services Roundtable, an advocacy organization for America's financial services industry. Prior to joining the Financial Services Roundtable, Governor Pawlenty served, as we know, as the Governor of Minnesota for two terms. We are happy to see you.

Our second witness is Sandra Kennedy. I have not talked with her since yesterday, and it is good to see you again this soon. She is President of the Retail Industry Leaders Association, the trade association for America's largest and most innovative retail brands. In this position, Ms. Kennedy works to promote the public policy interests of its members to ensure continued growth in the retail industry. Ms. Kennedy previously served as the Director of Leadership Dialogue Series for Accenture, a global management consulting and technology services company, and as the Senior Vice President of Member Services for the National Retail Federation.

Our final witness is Tiffany Jones. Ms. Jones is the Senior Vice President of Client Solutions and Chief Revenue Officer for iSIGHT Partners, a cyber threat intelligence firm, where she leads the de-

velopment of business strategies and field execution. Prior to joining iSIGHT Partners, Ms. Jones worked in senior roles at Symantec and served as Deputy Chief of Staff at the White House Office of Cybersecurity and Critical Infrastructure Protection. All I can say is you must have started really early in that work, early in your life.

All right. We are glad you are here. Your whole testimonies will be made part of the record, and feel free to summarize as you wish and then we will just have a good conversation.

Again, my charge to you, as it was to the first group, we talked enough about the different people's legislation, introducing legislation, the problem, why we need to do something. Everybody agrees we have to do something. There is a role for the private sector. There is a role for us here. What we have to do is figure out our role here, what to do, what not to do, so we need your help. I think this is, actually, two good panels to help us to accomplish those goals.

So, Governor, take it away.

TESTIMONY OF HON. TIM PAWLENTY,[1] CHIEF EXECUTIVE OFFICER, FINANCIAL SERVICES ROUNDTABLE

Mr. PAWLENTY. Chairman Carper, good morning, and thank you for the opportunity to appear here today to address the important topic of data breaches and the further steps needed to better protect personal information and the payment system from cyber threats. We appreciate your leadership and your concern and your commitment to these very important issues.

In my testimony this morning, I would like to address two major points. First, the financial services and retail industries are working together to aggressively address cybersecurity and the threat of cyber breaches. And second, and importantly, we cannot optimally address these challenges without congressional action, so we want to urge that, and I will touch upon that more in detail in just a second.

The financial service sector is better prepared than other sectors to defend and respond to cyber attacks, but we also have more work to do as these threats continue to evolve. We have the strongest information sharing process of any critical infrastructure sector. Industry-wide initiatives are underway to identify and take action on information sharing, tactical operations, stronger Internet controls, and more research and development. We also plan and run simulations to improve defense and resiliency.

As you know, financial institutions are also regulated and examined to ensure compliance with comprehensive data security, privacy protection, vendor management, and resiliency requirements. The financial service sector proactively works with the Treasury Department, regulators in government, and law enforcement agencies to improve cyber defenses. We also worked with the National Institute of Standards and Technology (NIST) as they developed the standards, and we support directionally, of course, the cybersecurity framework that was recently issued through the

[1] The prepared statement of Mr. Pawlenty appears in the Appendix on page 267.

NIST process. We do all of this because we owe it to our customers to protect them and to maintain and keep their trust.

You have already heard about and touched upon the scale and nature of the problems that our industry and the economy more broadly is facing, so rather than focus on that, I will focus on the future in the remainder of my time.

In the wake of the recent data breaches at Target and other places, Sandy Kennedy and I got together and decided it would be best for our consumers and for our industry to collaborate with our other industry partners to strengthen our defenses and keep the focus on the real enemy, our cyber attackers, and try to minimize the finger pointing back and forth about who could or should be doing what.

Chairman CARPER. And maybe we should take a lesson from that here. [Laughter.]

Mr. PAWLENTY. So, along with 17 other trade associations, Mr. Chairman, we established the Merchant and Financial Services Cybersecurity Partnership. That partnership overall has two major goals, first, to improve overall security across the entire payments ecosystem, and second, to bolster consumer confidence in the security of their data and the payment system overall.

The partnership consists of a number of things, but at core, it is five working groups that will focus on the following five topics: One, threat information sharing; two, cyber risk mitigation; three, advanced card present security technology; four, card not present and mobile security technology; and, five, cybersecurity and data breach notification.

Our progress, however, is going to remain inadequate unless we have some additional help in partnership with further actions needed from Congress.

Institutions need to have the ability and the necessary liability protections to share threat information with other private partners and the government when they act in good faith to defend consumers and the financial system.

As was mentioned, we also need robust data breach notification legislation setting a strong national notification standard. This standard should be clear so that customers can understand what happened and companies know what actions to take. These standards should be uniform so that customers can be treated similarly, regardless of what State they live in.

Mr. Chairman, your Data Security Act of 2014 and the Cyber Intelligence Sharing and Protection Act (CISPA), which was recently passed by the House, are both terrific efforts. We are very pleased with those efforts and we want to make sure that they advance and do all that we can to help you in your efforts to advance that legislation.

In the end, all of us, retailers, financial service companies, the government, want to stop attacks in real time and prevent them, and we also want to make sure that if in the event attackers do break through, that they find nothing of value and cannot leave our system with things of value.

Mr. Chairman, we believe the partnership between the retail industry and the financial service industry will help us get closer to achieving these goals. We will certainly keep you informed of our

efforts and our progress. We do not view this as a multi-year framework. We would like to get this up and running with results over the next 6 to 12 months.

And we also hope that the legislation that I referenced will pass the U.S. Congress. It is overdue. It is urgently needed. And we appreciate your efforts and leadership in that regard, and I certainly welcome any questions once the panel comments are complete.

Chairman CARPER. Great. Governor, thanks for those comments, and we appreciate your work on this and look forward to being your partner. Thank you. Ms. Kennedy.

TESTIMONY OF SANDRA L. KENNEDY,[1] PRESIDENT, RETAIL INDUSTRY LEADERS ASSOCIATION

Ms. KENNEDY. Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee, thank you for the opportunity to testify today before the Committee.

The Retail Industry Leaders Association (RILA) represents the Nation's largest and most innovative retailers. Together, our members employ millions of Americans, generate more than $1.5 trillion in annual sales, and operate more than 100,000 stores and distribution centers around the world.

I welcome the opportunity to talk today about cybersecurity threats we collectively face and steps that the retail industry is taking to address them in order to better protect our customers. I am pleased to be testifying alongside Governor Pawlenty, a person with whom I have developed a strong working relationship as we pursue this very important partnership.

The threat of cyber attacks is all too common. Though we place a premium on security, cyber criminals are persistent and their methods of attack are increasingly sophisticated. As we have seen, no organization, be it business, nonprofit, or government agency, is immune from attacks. Given the scale and impact of the threats, and with strong support of our Board of Directors, RILA launched a comprehensive initiative in January. The initiative is intended to enhance the industry's existing cybersecurity efforts, inform the public dialogue, and build and maintain consumer trust.

We have identified three main components relevant to today's hearing: Strengthening threat information sharing in cybersecurity; engaging with Congress on breach notification legislation; and collaborating to pursue enhancements to payment security.

There is widespread agreement that merchants should have had an information sharing mechanism through which retailers can communicate with each other about threats. To that end, RILA formed a council made up of the top security executives at our member companies. The council has formed a partnership with the National Cyber Forensics and Training Alliance, and we met last week at its headquarters to begin the important work of establishing a trusted forum. The forum will allow retailers to share threat information and collaborate with businesses and government agencies on solutions to combat cyber criminals. We have already begun to study the threat sharing model used by the financial serv-

[1] The prepared statement of Ms. Kennedy appears in the Appendix on page 273.

ices industry and believe there is a great deal that we can learn from that industry.

The initiative also calls on Congress to pass a national breach notification law. Following a breach, retailers secure their systems and make every effort to provide timely notification and actionable information to their customers. RILA urges that Federal breach notification legislation, one, preempt the State laws in place today; two, take into account the practical realities of notification, such as providing adequate time to secure the breached environment, investigate and analyze the breach, and comply with any law enforcement direction; and, finally, be proportional and linked to the risk of harm, be it financial fraud or identity theft.

We applaud Chairman Carper, Senator Blunt, and other Members of this Committee, for pursuing breach notification legislation. We want to work with you on a Federal bill that will be consistent with the goals I have outlined.

Finally, RILA's initiative recognizes the need to strengthen security within the electronic payment system. The initiative spells out near and long-term actions that can be taken to improve payment security, including retiring the magnetic stripe, adding PIN authentication to all credit and debit card transactions, migrating to chip and PIN cards, and collaborating on solutions to online, mobile, and other transactions where the physical card is not present.

While retailers believe these goals are reasonable, achieving them will be challenging and require substantive collaboration across the entire payments ecosystem. The need for collaboration was the genesis behind are partnership with Governor Pawlenty.

The tasks of these working groups, which Governor Pawlenty described, are significant, but we believe that they are achievable and we are committed to pursuing significant progress over the course of the next 9 to 12 months. While we expect there to continue to be issues on which we disagree, we have a shared obligation to consumers to find ways to improve payment security.

In closing, we believe by working together with public and private sector stakeholders, we can maintain the strongest defenses against cyber attacks and render stolen data largely valueless to cyber criminals.

Again, I very much appreciate this opportunity, Mr. Chairman, and welcome your questions.

Chairman CARPER. Thank you, Ms. Kennedy. Thank you.

Tiffany Jones, welcome. Please proceed.

TESTIMONY OF TIFFANY O. JONES,[1] SENIOR VICE PRESIDENT AND CHIEF REVENUE OFFICER, iSIGHT PARTNERS, INC.

Ms. JONES. Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, thank you for the opportunity. My name is Tiffany Jones. I represent iSIGHT Partners, a leading cyber threat intelligence firm. Over the last 7 years, we have built a team of over 220 experts dedicated to studying cyber threats in many nations across the globe and enabling organizations to protect themselves against these threats.

[1] The prepared statement of Ms. Jones appears in the Appendix on page 278.

There are a variety of different threat domains that make up the cyber threat landscape today. Each of these threat domains is motivated differently. For example, Cyber Espionage, targeted intrusion operations aimed at corporate and government entities to collect information for the purpose of strategic advantage, can be politically motivated or economically motivated. Cyber hacktivism focuses on the intentions and capabilities of politically or ideologically motivated actors. And then you have cyber crime focusing on cyber threats from primarily financial motivated actors.

The intelligence we research, analyze, and disseminate, coupled with the scope, scale, and duration of the recent retailer attacks, leads us to one very clear conclusion. We need to stop thinking about cyber crime like the movie, "*Catch Me If You Can*," one clever young man assuming identities and passing bad checks, and instead, we need to understand that cyber crime is more like the movie "*Goodfellas*," an organized community of bad people intent on crime, economically motivated, increasingly sophisticated, and operating without much fear of law enforcement.

Cyber crime is a global industry, with a division of labor. It involves supply chain as well as a defined value chain. This chart over here actually gives you an overview of what the value chain looks like.[1]

In step one, you have malware. Cyber crime starts with malware. Think of this like the App Store for hackers. Thousands of developers craft hacking tools and tool kits with various features, functions, and capabilities and then sell them in a broad array of electronic markets. Prices can range from a few to several thousand dollars. Just like an App Store, only a fraction of the malware goes on to be popular, depending upon the features, the targeted vulnerability, usability, and other characteristics. But at any point in time, there are probably a few thousand notable pieces of malware on the market, with 10 new entrants that warrant real analysis in a given month. At higher prices, subscriptions of $5,000 to $15,000 per month, there is also private access to malware developers. These are the more sophisticated designers.

Step two is the infrastructure. Cyber criminals must obfuscate their operations. This means buying, storing, computing, and network services from dedicated infrastructure operators. Think of criminal cloud computing. This is a large and varied segment of the market, everything from securing $50 domain names to $1,000 per server, per month hosting arrangements, and some of these organizations can scale to multi-million-dollar operations serving more than a thousand criminal clients at a time.

Step three is the cyber crime operators. Like entrepreneurs, operators assemble temporary teams, acquire tools, secure infrastructure, and execute against a plan. The better the plan, the bigger the payout. Like entrepreneurs, the very best exploit a market need, quickly monetize the value, and move to the next opportunity. In fact, one recent observation we have observed netted as much as $3.8 million for the operator and their team in just a couple of short months.

---

[1] The chart referenced by Ms. Jones appears in the Appendix on page 281.

Step four, the brokerages or intermediaries. To monetize stolen assets in cyber crime, typically, this is some form of personal data—credit card, health insurance, Social Security numbers, PII. The operators take that bulk data to brokers. Think of these players, again, numbering in the thousands, as wholesalers. The brokerages pay bulk prices to the operators for the stolen data and then parcel it up into sizes that a large number of smaller criminals can use. At the retail level, this looks like an underworld eBay with prices set by type, the newness, the quality, and the completeness of the stolen data. More reliable sellers get higher prices.

In early December, we saw complete U.S. credit cards at $100 per card. But with the dramatic increase in supply due to several recent retailer breaches, the price dropped to $50. Much of that card data is now dated and U.S. cards are selling closer to $16 per card.

Step five is the card buyers and mules. The transition from the criminal economy to the traditional economy presents the biggest bottleneck right now for cyber crime. Using stolen information involves risks and transaction costs, so most cyber criminals leave much of the small change on the table while focusing their efforts on the big quick hits. Card buyers and mules bear most of the risk. The typical card buyer or mule for receiving stolen property or bank payments is just a small time, sometimes even occasionally unwitting, criminal. Think of them as the intern of the cyber crime industry. They get relatively small payments for relatively small crimes. They are typically involved in the illegal activity for a short time and have no connection with the larger criminal enterprise. Like a pickpocket who just takes the cash from your wallet, their gain is small, but your loss in time effort and personal value can be significant.

So, as you can see, the scope of the cyber criminal market is daunting and the money made pales in comparison to economic value destroyed as a result. At any time, there are tens, if not hundreds of thousands of independent actors. They are global. They are unregulated. They are better equipped, better trained, and more experienced than many of their law enforcement counterparts, and they are growing bolder. You will see, like the 2013 retailer breaches, again, with greater frequency.

Business and government have started to understand the scope of the problem. They are increasingly shifting to an intelligence-led cybersecurity approach to improve prevention, speed response, and solve the cybersecurity risk equation. There is progress, but there needs to be more of it. Thanks to government entities like the Department of Homeland Security, U.S. Secret Service, and others, the severity and scope of the problem is becoming increasingly evident.

I will be happy to answer any questions that you have following our discussion here today.

Chairman CARPER. Thank you. Thank you all for good, helpful testimonies.

If you were here for the beginning of the first panel, I said to that panel—I quoted Abraham Lincoln. The role of government is to do for the people what they cannot do for themselves. And I asked them to help us figure out what the private sector can do in

this regard to protect information, money, things of value, particularly with respect to these breaches. But, what can the government do and what should the government do? And there is a broad range of views on what is the role of the government. We heard a little bit of that this morning.

But what I am trying to get at is consensus. If I had the first panel still here, I would put all of you up here and say, let us just go down the line and tell me where you think you agree. Tell me where you think you agree on what the government should do. What is our role? And let me just ask that, and Governor, I will ask you just to lead off. What is our role?

Mr. PAWLENTY. Mr. Chairman, I think there are a number of things the government can and should do, and we would urge you to take these actions. First of all, it is appropriate for your Committee to be focused on these issues. As was mentioned, many of these instances are not just transnational criminal elements, but we, of course, through public reports and otherwise, have reason to believe there is the prospect of cyber terrorism, self-declared cyber jihadists, and other elements that you would fall into the category of not just cyber criminal activity, but potential for cyber terrorism. So, obviously, your Committee is appropriately focused on these issues.

At a minimum, Mr. Chairman, we hope that the Senate and the Congress more broadly would take action promptly on the national data breach notification laws that will help in terms of the response to incidents, but we also should realize that that is just one step and an incomplete step. We also need to do all that we can to be better prepared and more resilient on the prevention side.

One thing that would help tremendously, Mr. Chairman, is if the Congress would pass an information sharing bill that would be similar, or at least directionally similar to the House CISPA bill. We realize that post-Snowden, that became more difficult, but we hope that post-Target, that that becomes more possible.

Again, we are, as an industry and our sector, in particular, are extraordinarily dedicated on these issues. Fortunately, the financial service sector has not yet experienced a large-scale successful attack, but we are greatly concerned about these issues and these challenges and we would be better prepared and could be better on the prevention side if Congress would allow that threat information sharing bill.

To give you one example, if we have reason to believe, good faith, a reason to believe that a certain entity or an Internet Service Providers (ISP) address is preventing threatening information and we move to constrain or shut off that ISP, even though we did it in good faith as a way to stop the contagion, if we do not have some protection around that action, if it is done in good faith for proper reason, we are going to be less likely to do that. If we are going to share threat information with another entity or the government and it is going to get the Freedom of Information Act (FOIA)-ed, it turns out to be not what we thought it was and we are going to get sued over that, or the entity is going to get sued over that, those are the kinds of things that are deterrents to more high-speed, more aggressive defensive mechanisms, and a bill like that would help, sir.

Chairman CARPER. OK. That is very helpful. Thank you. Ms. Kennedy.

Ms. KENNEDY. At the risk of being repetitive, Mr. Chairman——

Chairman CARPER. Repetition is good. [Laughter.]

This is one of those instances where repetition is good.

Ms. KENNEDY. We support Federal breach notification legislation, as well, and as you know, it is one of the working groups that the Governor and I will be working on with our fellow associations. It is important that such legislation creates a single national law that preempts the State laws so that we are not having to comply with a patchwork of 46 or 47 different State laws.

It is also important that notification be proportional to harm. If someone has stolen my shoe size or the type of cookies I like, that is one thing. If they have stolen my personal information related to my payment system, that is another. So, that is important to us, as well as making sure that it is reasonable given the operational requirements as well as those that are placed on us by law enforcement.

Chairman CARPER. Give us some—that word "reasonable" is going to be not an easy one to define. Just think out loud about what, when you say reasonable, what are you thinking?

Ms. KENNEDY. I am thinking that——

Chairman CARPER. Or maybe some examples.

Ms. KENNEDY [continuing]. It takes time for our members to identify the threat, to stop the threat, to assess the damage that has been done, and the data that has been stolen. And, of course, law enforcement has a role in that. So, I think it is important that that is all considered in terms of the practicality of the legislation.

Chairman CARPER. OK. Ms. Jones, same question.

Ms. JONES. A couple of "don't"s and then a couple of "do"s.

Chairman CARPER. Umm, I like that.

Ms. JONES. Do not seek to be technically prescriptive, so——

Chairman CARPER. Chip and PIN. It is not our job to say——

Ms. JONES. So, chip and PIN, I will say, does increase security, absolutely, so if there is any question about that it does. But it is not the panacea. And so——

Chairman CARPER. Is it our role to prescribe that? I think not.

Ms. JONES. I do not think so. But I do think it is absolutely in your authority to look at the overall standards and make sure that they equate to the threat that is today, all right.

Chairman CARPER. Someone said to me, they said, if you want to go ahead and prescribe chip and PIN, you can do that, but the threats change, technology changes. He said that to me, if you have not noticed, sometimes it is hard to get Congress to move, and we need to be able to move a lot faster.

Ms. JONES. Yes, and our information technology is dynamically changing, as well. And so today's cool thing is going to be tomorrow's, oh, that was so yesterday, right. So, I think there are other things to consider. I would say, think about it in the sense of do all that you can to deter the bad guys from getting in, but also, assume that they are in. How do you protect the data, assuming that the bad guys are in the environment? So, things like encrypting data at rest, encrypting data in transit, those types of things are also really important to think about.

Chairman CARPER. What was the first thing you said, encrypting data at rest? What does that mean?

Ms. JONES. Correct. So, if it is just sitting there in a server, in a storage space, in a data center within an organization's environment, it is sitting there at rest. And in many cases for a lot of organizations today, they actually are only encrypting data as it is being transferred from their environment to another organization or environment. That is data in transit. So the data at rest is simply when it is just sitting there within their organization. Is it being properly protected?

Chairman CARPER. OK.

Ms. JONES. And then, do not equate the quantity of arrests in cyber crime with the quality of arrests. Focus prosecution higher in the value chain. It makes a significantly bigger impact. And, again, I applaud the work of Secret Service and DOJ and what they are doing there. I think they are making the right steps, for sure.

I would say on the "do" side, do increase global collaboration. Most of these people, these threat actors, are not inside our borders, and so that global collaboration among law enforcement is absolutely critical.

And do pass national data breach legislation. It was said quite eloquently, there is a patchwork of State laws. I think of my mother and I think of, why does it matter what State she lives in to determine the level of protection that she has? It should not.

Chairman CARPER. Where does your mother live?

Ms. JONES. She lives in Illinois.

Chairman CARPER. OK. Well, if things get too hot there, she is always welcome to come to Delaware.

Ms. JONES. Delaware. [Laughter.]

Chairman CARPER. And when it gets hot, people will come to Delaware and they will go to our beaches. We have, I think, more five-star beaches than any——

Ms. JONES. They are beautiful.

Chairman CARPER [continuing]. Any State in the country. We are very proud of them. But, one of them is Rehoboth Beach. Rehoboth translates literally, Governor, and means room for all. Is that not nice? Room for all.

All right. Some of you said very nice things about the legislation that Senator Blunt and I have introduced. I like to say, everything I do, I know I can do better. I think that is true of all of us. It is certainly true of the Federal Government, Federal agencies. But not everyone appreciates every aspect of our bill and I would just invite you to—you have heard some of the criticisms of each of the major pieces that have been introduced in the Senate. But just share with us some of the criticism, whether they are legitimate or not, of our legislation. And if you think those are reasonable criticisms that should be addressed in modifying our legislation, fine. I would like to hear that. If some of the criticisms, you think, are just not very well founded, not very well thought out, then help us rebut those. If you could do that, that would be much appreciated.

Do you want to go first, Ms. Jones.

Ms. JONES. I have no criticisms on the legislation——

Chairman CARPER. But maybe criticisms that you have heard, because I read some articles where folks have taken some big potshots at the handiwork of Senator Blunt and myself.

Ms. JONES. I think one of the criticisms, in general, for not wanting to pass national data breach legislation has simply been that you create a baseline that is so low, maybe there are certain State laws today that have higher levels of protection for their consumers. But, I counter that simply with just having a consistency across the Nation is more important for the consumer than the patchwork. And the amount of money that companies are spending today just on compliance is pretty unbelievable to deal with the various State laws. So, I think it is really important that they can reinvest their dollars that they are spending in compliancy today and actually put it into information security protection.

Chairman CARPER. OK. Thank you.

Ms. Kennedy, what are some of the criticisms you have heard of our bill that you think are reasonable, should be incorporated, maybe some that are less thoughtful, and rebut those. Rebut those for us, if you could.

Ms. KENNEDY. I think that as we looked at your legislation, we certainly support the preemption and the recognition that businesses have practical operational areas they need to address before they do notification.

We would welcome the opportunity, I think, to talk to you about enforcement, to make sure that the FTC has very clear direction on what enforcement looks like. And that is——

Chairman CARPER. All right.

Ms. KENNEDY. Otherwise, we are in agreement with a number of things in your bill.

Chairman CARPER. Governor Pawlenty.

Mr. PAWLENTY. Mr. Chairman, I would echo those comments and just say there has been some criticism, not by us but by others, on the standard that is set in terms of substantial harm and inconvenience to the consumer. We think that standard strikes the right balance. Obviously, it is going to be interpreted, and so some others have expressed concern about that, but we just reinforce that we think that you and Senator Blunt have struck the right balance in that regard.

If I might, Mr. Chairman, just for a second jump back to the issue around mandating technology, for all the reasons that were mentioned by Ms. Jones, we concur with that. Keep in mind that there are—as cards get misused, there are fraudulent or forfeited cards, and, of course, the chip protects the security of the card and so it cannot be forfeited or it would be much more difficult to forfeit. And then the PIN authenticates the user, or a signature does, or in some cases of small transactions, no signature.

So, technology in the payment space is going to continue to evolve. It already is evolving rapidly. But also, keep in mind that relates to card present environments, and as commerce continues to migrate to the virtual space and e-commerce platforms, there is a whole another set of concerns and issues and opportunities around something called tokenization, secure cloud transactions in the space that will address the card not present environment that is important to the discussion, as well, because if you make it much

more difficult for the fraud to occur at the card present environment, it will shift to the card not present environment and we need to do both.

Chairman CARPER. All right. Thank you. Card not present—that is one I just learned this week. I hear all these new terms. No wonder my colleagues and I have a hard time figuring out what to do here. It can get pretty confusing.

One of the things you are trying to do with this new partnership, though, Governor and Ms. Kennedy, is to try to take some of the obligation or the work that needs to be done off of our plates and really put it where it better belongs, and that is on yours. But we are pleased to see people like you and the folks you represent working together on these issues, and the new partnership certainly seems on its surface to be a step in the right direction. We would like to hear just a little bit more about it before we close, and if you maybe could just share with us some of the goals that you see.

Mr. PAWLENTY. Sure.

Chairman CARPER. These are the goals that we have for this partnership, and maybe give us a snapshot of the timeline for the group, please.

Mr. PAWLENTY. Sure. Well, again, I want to tip my cap to Sandy Kennedy and her leadership in the Retail Industry Leaders Association. They came forward on behalf of that sector and have been extremely constructive and forward leaning on these issues.

We have said, to your 80/20 comments earlier, there is some stuff we are not going to agree on about card replacement costs and some of the fallout of these previous breaches. That is going to get litigated and settled, hopefully, in another forum. But, there is a lot of stuff we can agree on, so we are focused on that, and we think we can agree and hope to agree on these things.

One, come together with a statement of principles, maybe even a specific statement of support on national data breach notification legislation.

Two, make sure that we do all that we can to agree upon and advance cybersecurity information sharing legislation.

But on the things we can do ourselves, we have realized even in the early inventory of practices, government to industry, industry to industry, that there is a lot that this partnership can share without government mandating a requirement on technology best practices, cyber best practices, cyber defenses, resiliency, simulations, sector coordinator councils, and much more. So, we can get that done.

And then, last, there has not really been a good forum for various players in the payments ecosystem—retailers, card issuers, merchant acquirers, financial institutions, the banks on the other end of the transaction, various other cyber entities—coming together to talk about, can we agree on where we are headed in the so-called Europay, Mastercard, and Visa standard (EMV), card present, card not present, next steps on technology and cyber defenses.

So, at the very least, we hope we can convene that discussion, but we believe that out of that discussion we can agree on some next steps that will be very important and helpful, and our timeline is 6 to 9 months, Mr. Chairman.

Chairman CARPER. OK. Thanks. Ms. Kennedy.

Ms. KENNEDY. I would just like to elaborate a little bit on the working groups. As I mentioned, they are comprised of executives from both the financial services as well as from our merchant members and they have clear objectives. We are working with people to help keep us on track, project management. They have clear deliverables, and they are going to be challenging deliverables, but we think that it is important for our shared customer that we deliver on those.

I would also like to say that this has been a very welcome partnership. The payments system is an ecosystem and you have to have all the links in place and everyone as strong as they can be. So, we are going to learn a lot, I think, from our partners, and I think that we are also going to have an opportunity to address the future issues that we are going to face. The way our customers are shopping are changing every day, whether it is mobile or it could be wearable technology. I mean, they are adapting so quickly. So, it is very important that the payment system keep up with that so that confidence is maintained with our customers and they continue to shop with us.

Chairman CARPER. OK. The words "information sharing" have been mentioned a time or two on this panel, and I think even on the first panel, and I am not sure—Governor, I think it might have been you who mentioned what we might need to do to facilitate information sharing. Can you just drill down on that for me a little bit, please.

Mr. PAWLENTY. Sure, Mr. Chairman. One of your previous witness on the panel before us made reference to a recent study that I think is worth just camping on for a minute. The Washington Post recently reported that the Federal Government notified 3,000 businesses last year that they were breached, and the Verizon study indicated that 70 percent of those companies did not know they were breached until the Federal Government told them.

So, when you think about these issues from a Federal Government knowledge standpoint and capacity standpoint, of course, that knowledge resides, oftentimes, in the FBI, Secret Service, Department of Defense, the National Security Agency (NSA), Homeland Security, Treasury, and others. So, there is an opportunity and a challenge to better integrate and coordinate intergovernmental information sharing and it is not optimized at the moment. But then, also, there is a need for that information to flow to the private sector in appropriate ways, respecting privacy rights.

The FS–ISAC, and I know the Financial Services Sector Coordinating Council (FSSCC) which you are speaking to later today, are examples of portals between government and the private sector that allow that information to flow. But, unless we have the legal changes that I mentioned earlier that provide those protections for information sharing done in good faith—again, threat information, not personal information—we cannot move this to the place that it needs to go. And so that is really needed and it is really helpful and it is one of the best things that we can do. The NSA, for example, is viewed by many as the best entity when it comes to cyber and they were breached. They had a massive breach, internal, insider threat. It crossed numerous platforms.

So, the point is, the government has great knowledge they can share with private industry, but private industry, if one of our members shares it with the government and then it becomes a FOIA request and you have knowledge that is proprietary and/or you misstate something, even though it is done in good faith, the lawyers get a hold of that, class action suits start, regulators might want to be interested in that. Unless you have some rules of the road going into that, you are going to be less likely to share the information lest you know what is going to happen to it.

Chairman CARPER. All right. Ms. Kennedy, as you know, in this Committee, we work a fair amount on cybersecurity. We work on other things, too. But particularly with the defensive side, we often hear that technical collaboration and information sharing are essential parts to a strong cyber defense. Talk to us just a little bit here on information sharing, and I am going to give you a chance to ask you to come back and just revisit it with us here again, but do you think that the recent series of breaches has impacted the level of information sharing between companies, the willingness to share information between companies, the willingness to share information with, we will say, law enforcement, with Federal agencies?

Ms. KENNEDY. Absolutely, Mr. Chairman. We think it is imperative, and it was really key to our initiative that was approved by our Board of Directors, and we have already started that process. I think information sharing has been occurring within our industry, but we think it is important that we formalize that in some way and we are looking at different ways to do that now. We had, I believe, 30 of our member companies in Pittsburgh last week for a meeting where that was one of the central discussions, of how we can effectively share information to make sure that we are doing all that we can to protect our customer.

Chairman CARPER. OK. Ms. Jones, are you up for one more question?

Ms. JONES. Absolutely.

Chairman CARPER. OK. This is really more of a focus, I guess, for law enforcement, but we will deputize you——

Ms. JONES. Thank you.

Chairman CARPER [continuing]. And ask you to step up to the plate. But, I think in your testimony, you provide a fair amount of background on the criminal networks that are often behind the data breaches that we are talking about here today. I was especially interested to learn about all the different steps that are needed to monetize the personal information that is stolen from an organization.

And before I ask the question, as it turns out, one of the credit card banks that is involved in the Target breach is TD Bank and their credit card operation is in Wilmington, Delaware. We actually visited with them, and this was a month or so ago. We are interested in learning just how most of the losses are absorbed, I think, by banks, not by the merchants in these cases—trying to just get them to give us a sense for how much money was at stake here and at risk here to be lost. And I was struck by one of the things they said, and I think we heard it here, as well.

The folks who actually figured out how to get in and steal the data or the information from Target were pretty good at doing that. They were less adept at monetizing and figuring out, once they had all this information, what to do with it and an effort to make money. The banks reacted very quickly. They immediately sent out to people like me new credit cards and responded. There is a lot of cost to this stuff, I am sure. But, the losses were, I think, a good deal less than certainly I ever expected them to be. And, again, the reason that was explained to me, they are better at stealing the data than actually monetizing, which is a good thing. It is a good thing.

Where in the process are cyber criminals most vulnerable? In other words, where in the process should U.S. law enforcement be targeting our limited resources? This is something Dr. Coburn talked about quite a bit.

Ms. JONES. Yes, absolutely.

Chairman CARPER. Go back and revisit that.

Ms. JONES. So, pertaining to where law enforcement needs to focus, I think as I had talked about the ecosystem, lots of different players, loosely affiliated, or highly organized crime cells, I think you have to move up into the supply chain. Do not be going after the mules, necessarily, the small petty theft folks. I mean, yes, you want to try to gather all that you can and go after them all, but if you have limited resources, you really want to go after the highly organized kind of crime organizations that are really ultimately trying to monetize all of this, right.

The operators, the infrastructure providers, they are just small pieces in all of this. Now, if you can start going after different points in the supply chain, you are going to get further along. But, ultimately, you get one infrastructure provider, pull him away, another will show up, because the demand is there. It is very low cost overall and low skill to establish those capabilities. You just have to have the resources to go buy them.

Chairman CARPER. OK. The last question is, we asked you to give an opening statement, and sometimes, if we have time, I like for our witnesses to give us a closing statement, especially when we are trying to develop consensus on an issue about which there is not absolute consensus. You can take advantage of this opportunity if you would like and give us a short closing statement. But if you have something you want to reiterate, a point that has been made, something that one of your colleagues has said that sort of triggered a thought, that would be fine, as well. But, just a very brief closing statement, maybe a minute or so.

Mr. PAWLENTY. Just very briefly, Mr. Chairman, thank you again for your leadership and your commitment to these issues.

I would just try to impress upon you and the Committee a sense of urgency. The nature and sophistication and pace of these attacks is evolving daily, weekly, and it is concerning. And I hope that we do not find ourselves a year from now or 2 years from now waking up to a bigger problem, wishing action would have been taken earlier.

So, if I were to just emphasize one theme, it would be a sense of urgency. As the threat increases, the pace of response needs to

increase from us, from our partners, and, candidly, from the Congress.

Chairman CARPER. Good. Thank you. Ms. Kennedy.

Ms. KENNEDY. Cybersecurity is a top priority for the retail industry, and we are working in an ecosystem. The data that has been stolen was payment data, so it is important that we have our partners on board and it appears that we are going to make some great progress in that area.

I think it is also important in this ecosystem to understand that we also share in the loss, share in the fraud. The Federal Reserve, in fact, puts it at almost 50/50. So, as we look at this, we all have a stake in this game.

Chairman CARPER. Good. We all have a dog in this fight.

Ms. KENNEDY. We do.

Chairman CARPER. Yes. Ms. Jones.

Ms. JONES. Everybody is using the term "cybersecurity" as the buzz term of the day, but at the end of the day, what this is is just simply a risk management problem, like many problems out there today. But, we are not treating it like a risk management problem, typically. We are typically treating it like, let us throw more technology at the problem.

And I think one of the things that we are recognizing in speaking—I am going around the country, speaking to a lot of retailers right now who have lots of questions—they are really trying to wrap their arms around, what is the threat? They actually do not have a good sense for their threat profile, many of these companies. And so you cannot solve for risk if you do not understand the threat profile.

So, I would say, as we look at things like the NIST framework that I know there has been a lot of work that has gone into, making sure, threat is really brought in more effectively into the risk equation is going to be critical. Otherwise, we are continuing to solve for vulnerability mitigation.

Chairman CARPER. Well, that is a good note to end on.

About a year ago, a fellow named Pat Gallagher sat right where you are sitting and he is now the Deputy Secretary of Commerce. But, for a while, he was the person—in fact, he may be double-hatted, I do not know, dual-hatted, and still running NIST. But, he sat right there where you sit and he said in his testimony, we will know we are in the right place in this arena when good cyber policy is synonymous with good business policy. That is what he said. We will know we are in the right place when good cyber policy is synonymous with good business policy and where the government has less of a need to, like, to command and control, to dictate, whether it is technology or best practices and so forth. But when the folks that are either controlling the critical infrastructure, our merchants, our banks, whatever, when good cyber policy is good business policy, we will know we are in the right place.

I think we are actually moving in that direction, of which I am pleased. I think Pat and the folks at NIST did a very nice job working on the framework. I call it a blueprint or a roadmap. They got a lot of good support, a lot of good input, including from the folks at the table here and your member organizations, and we are grateful for that.

One of the other things I learned from that effort is, we will say on the day that the framework was put out there, best practices, it was out of date, because the nature of the attacks change all the time and we continue to have to evolve. It has to be a dynamic framework, if you will, dynamic blueprint, and we will seek to do that.

I think we will probably wrap it up here. This has been helpful, and we are going to be calling on you some more as Dr. Coburn, he said he is going to leave us at the end of the year, cutting his term short by 2 years, and I said—and he said he wants to finish strong. I want him to finish strong. I want us to finish strong and this would be a great area for not just the two of us to collaborate with John McCain and with Roy Blunt, but also Pat Leahy, Senator Leahy, with Jay Rockefeller, with John Thune and with Pat Toomey, all of our colleagues, Democrat and Republican, working with a lot of folks like you. And we look forward to doing that.

I am going from here to a luncheon, not a cyber luncheon, but a luncheon that Senator Reid, our Majority Leader, hosts every couple of weeks of Committee Chairs, and the first thing on our agenda is going to be to talk about this issue, data breach, and maybe how can we collaborate, how can we communicate, and how can we find principal compromises that advance the security of our Nation's citizens and our businesses.

With that, the hearing record will remain open for 15 days. I think that is until April 17, at 5 p.m. for the submission of statements and questions for the record. I suspect you will have some, and we would very much appreciate your responding to them in a timely way.

Again, thank you all very, very much.

And with that, this hearing is adjourned.

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

APPENDIX

Opening Statement of Chairman Thomas R. Carper
Data Breach on the Rise: Protecting Personal Information from Harm
April 2, 2014

As prepared for delivery:

I would like to begin by thanking our panel of witnesses for joining us this morning to discuss a critical issue that is facing our nation. I'd also like to thank Senator Roy Blunt for joining us today to discuss his work on this issue.

There is no doubt that technology has evolved rapidly, particularly over the last decade. And these advances will continue to grow exponentially in the coming years. Technology that, 10 years ago, could have been something out of a science-fiction movie, is now a part of our daily lives.

As we embrace the latest technology both at home and in the workplace, there is little doubt that more of our sensitive personal information is at risk of being compromised. Whether it is stored on the electronic devices we use daily or on a company server, this data can be vulnerable to theft.

As the way we communicate and do business has evolved, so have the tactics used by criminals to steal our money and personal information. Today's cyber criminals run sophisticated operations and are discovering how to manipulate computer networks and make off with troves of personal data. These data breaches have become much more prevalent, with a new one seemingly being reported almost every day.

Data breaches can put our most valuable and personal information at risk, causing worry and confusion for millions of individuals and businesses. The impact of a data breach on the average American can be extremely inconvenient and sometimes results in serious financial harm. Data breaches can also be extremely expensive for banks and other entities to respond to and remediate.

Although several high-profile retailers have recently become the face of data breaches, they are not the only victims of these cyber intrusions. Hackers are targeting all types of organizations that people trust to protect their information – from popular social media platforms to major research universities. The pervasiveness of these incidents highlights the need for us to find reasonable solutions to prevent attacks and protect consumers and businesses if a breach occurs.

We will hear in testimony today that many retailers, financial institutions, payment processors and the groups representing them are coming together to find common sense solutions that the private sector can undertake proactively without the help of Congress. These are groups which often times find themselves on different sides of an issue.

I recognize though that there remain existing areas where Congress can and should play a constructive role. One important area where Congress can play a constructive role is answering the calls for implementing a uniform national notification standard for when a data breach occurs.

Currently, when a breach happens, notification occurs under a patchwork of 46 different state laws. While some of these laws may have common elements, creating a strong uniform standard will allow consumers to know the rules of the road and allow businesses to invest the money saved from compliance into important upgrades and protections.

That's why I have joined with Senator Blunt to introduce the Data Security Act of 2014.

This common-sense legislation would require a national standard for entities that collect sensitive personal information. It would require these entities to enact a cohesive plan for preventing and responding to data breaches, plans that would detail steps that will be taken to protect information, investigate breaches and notify consumers. I've referred to these steps with the acronym P-I-N.

Most importantly, these plans would provide consistency throughout the nation and allow consumers to have a greater level of confidence that their information will be protected, and that they will be notified if a breach occurs despite whatever protective measures have been put into place.

We are never going to be able to prevent every breach, but we owe it to the consumers and the businesses and other entities that have been and will be victims of breaches to put into place the best system possible to deal with this growing threat.

I look forward to hearing from our witnesses today who are the leading voices on cybersecurity and data breach in both government and the private sector. I am sure their insight will be valuable as we continue with our efforts to fix this problem.

I am encouraged that many of my colleagues share my interest in advancing our efforts to address data breaches. I hope we can embrace the 80-20 rule. That is -- set aside the 20 percent that we can't agree on and focus on the 80 percent on which we can agree.

It is in everyone's interest to ensure that we minimize the occurrence and impact of data breaches.

###

Opening Statement of Sen. Tom Coburn, MD
Ranking Member
Homeland Security and Governmental Affairs Committee
Hearing on Data Breaches
April 2, 2014

Welcome, Sen. Blunt, and all of our witnesses here today. I would particularly like to thank Mr. Greg Wilshusen from GAO for appearing as the minority witness to discuss the federal government's challenges with cyber security and data breaches.

Data breach incidents are a serious problem. When we see examples like the Target data breach, with millions of people's personal information exposed, it is clear that our businesses need to do a better job protecting their customers' information.

I am open to legislation that would streamline data breach rules. However, we need to be careful to not be too prescriptive or punitive against companies. I look forward to learning more about Sen. Carper and Sen. Blunt's bill today.

We shouldn't lose sight of our responsibility to oversee the Federal government's data protection efforts. This Committee has clear jurisdiction over federal cyber security. I would like to take this opportunity to formally request that the next hearing this Committee holds on cyber security focus on federal cyber security and whether agencies are doing all they can to protect our sensitive information.

The American people don't have a choice but to give the Federal government their information. They don't have a choice but to submit their tax records every year to the IRS. They don't have a choice but to participate in the Social Security system. And now many don't have a choice but to sign up for HealthCare.gov. That data is no more secure in the federal government than in the private sector, and probably less so, in many cases.

Just as Target and other companies have a responsibility to protect their customers' information, the Federal government has a responsibility to protect the sensitive information it manages.

Too often, the Federal government fails to practice good cyber security.

Consider some examples: Last July, hackers stole the private information of 100,000 people from the Department of Energy. In 2012, the Thrift Savings Plan experienced a data breach that jeopardized 123,000 of their account holders' information. And earlier this year, the Department of Homeland Security exposed financial information and private documents that belonged to organizations that were bidding for contracts with the DHS Science and Technology (S&T) Directorate.

OMB and the Department of Homeland Security need to do a better job managing Federal cyber security. The GAO has done good work auditing federal cyber security, and identifying the many challenges that we face. I am happy that Mr. Wilshusen of GAO can join us today to speak to these problems and how we can fix them.

The Department of Homeland Security also needs to do a better job with its programs for Federal cyber security. Just today, the DHS Office of Inspector General released an important report looking at DHS's Einstein program.

Einstein is supposed to be the federal government's intrusion and prevention system for federal agencies. The DHS OIG identified a number of problems, including that the Department is not adequately monitoring the program's implementation and its handling of personally identifiable information.

The Inspector General reported: "There is little assurance that NPPD would be able to deliver intrusion prevention capabilities to participating agencies on

schedule." This is a key system that DHS views as the solution to protecting federal networks, and apparently it is not being managed effectively.

We also need to ask whether we are focusing on the right priorities for our cyber security spending. I welcome Mr. Noonan from the Secret Service today, and I look forward to his testimony. I am interested to know just how many resources we have devoted to investigating cyber crime and arresting the criminals who are stealing our information.

I am concerned we are spending most of the federal cyber security resources at DHS on vulnerability mitigation, and just a fraction on US Secret Service and FBI agents who are catching cyber criminals. Investigating and arresting cyber criminals is one of the best ways that we can deter cyber crime and protect our information.

We need to focus more on that kind of deterrence.

U.S. Senator Roy Blunt (Mo.)
Opening Statement, U.S. Senate Committee on Homeland Security & Government Affairs: "Data Breach on the Rise: Protecting Information from Harm."
April 2, 2014

Thank you to my friends, Chairman Carper and Vice Chairman Coburn for holding this hearing, and for inviting me to attend.

The problem of data breaches and notification to consumers is one Missourians are following closely.

This is an issue I've been working on for years. It's time for Congress to act to strengthen our nation's data security and defend consumers against breaches by both businesses and government agencies.

I'm proud to join my friend and colleague, Tom Carper, the Chairman of this committee, on bipartisan legislation.

In January, we introduced the Data Security Act to create consistent, national guidelines to better protect consumers from identify theft and account fraud in the first place – and to notify consumers in the event of a breach.

I'm also proud to cosponsor a similar bill introduced by Senator Toomey.

Identity theft is now the number one complaint to the Federal Trade Commission, and the criminals who perpetrate these acts aren't going away.

What the Data Security Act does is provide clarity – clear lanes in the road so that businesses, government agencies, and consumers can know what to expect in the event of a breach.

It's pretty simple: if a financial institution, retailer, or federal agency determines sensitive information was or may have been compromised, the bill requires them to investigate the scope of the breach and determine whether the information will likely be used to cause harm or fraud, and then notify law enforcement, appropriate federal agencies, consumer reporting agencies, and consumers themselves affected by the breach.

Federal legislation must be geared toward greater clarity – not complexity.

As things stand now, 49 states, U.S. territories, and the District of Columbia have different approaches to data security and breach notification. This confusing patchwork is bad enough, but now we're seeing some states revising their statutes in recent years, making things even more complicated.

The inconsistent patchwork of state laws creates a burden of compliance for companies – a burden that draws resources away from better security in the first place. I'm pleased that all the sectors I've met with agree on the need for a single federal standard on breach notification.

In a recent statement, Attorney General Eric Holder urged Congress to enact a uniform, consistent standard for notifying consumers about breaches. He said this "would empower the American people to protect themselves if they are at risk of identity theft" and "enable law enforcement to better investigate these crimes."

Last week, the Senate Commerce Committee held a hearing data breach notification. We had witnesses from virtually every sector: the Federal Trade Commission, the insurance industry, retail, credit cards, and even a university witness. I asked each of them whether a consistent national standard would benefit consumers, and each answered unequivocally: "Yes."

The cyber environment represents the fastest evolving technology in human history, and shifting standards that vary from one state or jurisdiction to another will only create more confusion.

I believe there is an emerging consensus in Congress that a consistent national standard for breach notification is the only approach that makes sense for consumers.

We need to acknowledge that hackers aren't going away. Our goal must be to clarify the complicated patch work of laws. Missourians and people across the country are counting on us to get this done, and I'm proud to be working in a bipartisan way to provide consumers with the protection and clarity they deserve.

Thank you.

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Breach on the Rise: Protecting Personal Information From Harm

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

Washington, D.C.

April 2, 2014

I. INTRODUCTION

Chairman Carper, Ranking Member Coburn, and members of the Committee, I am Edith Ramirez, Chairwoman of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on data security, and for your leadership, Chairman Carper, on this important issue.

Consumers' data is at risk. Recent publicly announced data breaches[2] remind us that hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses. These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information.

Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud, identity theft, and other harm, along with a potential loss of consumer confidence in the marketplace. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012.[3]

---

[1] This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] *See* Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times, Jan. 10, 2014, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html (discussing recently-announced breaches involving payment card information by Target and Neiman Marcus); Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, N.Y. Times, Jan. 25, 2014, *available at* http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html (announcement of potential security breach involving payment card information).

[3] *See* Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

As the nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement, education, and policy initiatives. The Commission is here today to reiterate its longstanding, bipartisan call for enactment of a strong federal data security and breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress must act. This testimony provides an overview of the Commission's data security efforts, and restates the FTC's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

The Commission enforces several statutes and rules that impose obligations upon businesses to protect consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for non-bank financial institutions.[4] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[5] and imposes safe disposal obligations on entities that maintain consumer report information.[6] The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online.[7] Reasonableness is the foundation of the data security provisions of each of these laws.

---

[4] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

[5] 15 U.S.C. § 1681e.

[6] *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[7] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.[8] A company acts deceptively if it makes materially misleading statements or omissions.[9] Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims about the security they provide for consumers' personal data. Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[10] The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[11]

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission's 50 settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.[12] And they have addressed the risks to a wide variety of consumer data, such as Social Security

---

[8] 15 U.S.C. § 45(a).

[9] *See* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[10] *See* Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

[11] Some of the Commission's data security settlements allege both deception and unfairness, as well as allegations under statutes such as the FCRA, GLB Act, and COPPA.

[12] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms.

In each of these cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

In its most recent cases, the FTC entered into settlements with Credit Karma[13] and Fandango[14] to resolve allegations that the companies misrepresented the security of their mobile applications ("apps"). Credit Karma's mobile app allows consumers to monitor and access their credit scores, credit reports, and other credit report and financial data, and has been downloaded over one million times. Fandango's mobile app has over 18.5 million downloads and allows consumers to purchase movie tickets. According to the complaints, despite claims that the companies provided reasonable security to consumers' data, Credit Karma and Fandango did not securely transmit consumers' sensitive personal information through their mobile apps. In particular, the apps failed to authenticate and secure the connections used to transmit this data, and left consumers' information vulnerable to exposure – including Social Security numbers, birthdates, and credit report information in the Credit Karma app, and credit card information in the Fandango app. The Commission's settlement agreements prohibit Credit Karma and Fandango from making misrepresentations about privacy and security, and require the companies

[13] *Credit Karma, Inc.*, No. 132-3091 (F.T.C. March 28, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.

[14] *Fandango, LLC*, No. 132-3089 (F.T.C. March 28, 2014) (proposed consent agreement), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.

to implement comprehensive information security programs and undergo independent audits for the next 20 years.

The FTC also recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.[15] The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

The FTC also has brought a number of cases alleging that unreasonable security practices allowed hackers to gain access to consumers' credit and debit card information, leading to many millions of dollars of fraud loss.[16] The Commission's settlement with TJX provides a good example of the FTC's examination of reasonableness in the data security context.[17] According to the complaint, TJX engaged in a number of practices that, taken together, failed to reasonably protect consumer information. Among other things, it (1) failed to implement measures to limit

---

[15] *TRENDnet, Inc.*, No. C-4426(F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[16] *See, e.g., Dave & Buster's, Inc.*, No. C-4291 (F.T.C. May 20, 2010) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; *DSW, Inc.*, No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; *BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter.

[17] *The TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.

wireless access to its stores, allowing a hacker to connect wirelessly to its networks without authorization; (2) did not require network administrators to use strong passwords; (3) failed to use a firewall or otherwise limit access to the Internet on networks processing cardholder data; and (4) lacked procedures to detect and prevent unauthorized access, such as by updating antivirus software and responding on security warnings and intrusion alerts. As a result, a hacker obtained tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. As this matter illustrates, the FTC's approach to reasonableness looks to see whether companies have implemented basic, fundamental safeguards that are reasonable and appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operations, and the cost of available tools.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, the FTC hosts workshops on business practices and technologies affecting consumer data. The FTC is in the midst of hosting its Spring Privacy Series to examine the privacy implications of a number of new technologies in the marketplace.[18] The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined the privacy and security implications of mobile device tracking, where retailers and other companies rely on technology that can reveal information about consumers' visits to and movements within a location.[19]

---

[18] Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues*, Dec. 2, 2013, *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

[19] *See* Spring Privacy Series, *Mobile Device Tracking*, Feb. 19, 2014, *available at* http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

In November, the FTC held a workshop on the phenomenon known as the "Internet of Things" – *i.e.*, Internet-connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumers.[20] The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas as diverse as smart homes, connected health and fitness devices, and connected cars. Commission staff is developing a report on privacy and security issues raised at the workshop and in the public comments.

And last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.[21] As the use of mobile technology increases at a rapid rate and consumers take advantage of the technology's benefits in large numbers, it is important to address threats that exist today as well as those that may emerge in the future. The forum brought together technology researchers, industry members and academics to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from potential security threats.

C. Consumer Education and Business Guidance

The Commission is also committed to promoting better data security practices through consumer education and business guidance. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[22] OnGuard Online and its Spanish-language counterpart, Alerta en Línea,[23] average

---

[20] FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), *available at* http://www.ftc.gov/bcp/workshops/internet-of-things/.

[21] FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), *available at* http://www.ftc.gov/bcp/workshops/mobile-security/.

[22] *See* http://www.onguardonline.gov.

more than 2.2 million unique visits per year. Also, for consumers who may have been affected by the recent Target and other breaches, the FTC posted information online about steps they should take to protect themselves.[24]

The Commission directs its outreach to businesses as well to provide education about applicable legal requirements and reasonable security practices. For example, the FTC widely disseminates its business guide on data security,[25] along with an online tutorial based on the guide.[26] These resources are designed to provide a variety of businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. First, companies should know what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs, so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas – physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly

---

[23] *See* http://www.alertaenlinea.gov.

[24] *See* Nicole Vincent Fleming, *An Unfortunate Fact About Shopping*, FTC Consumer Blog, http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping (Jan. 27, 2014); Nicole Vincent Fleming, *Are you affected by the recent Target hack?*, FTC Consumer Blog, https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack. In addition to these materials posted in response to recent breaches, the FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information. *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[25] *See Protecting Personal Information: A Guide for Business*, *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

[26] *See Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, *available at* http://business.ftc.gov/multimedia/videos/protecting-personal-information.

dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[27] For example, because mobile apps and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.[28] The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer ("P2P") file-sharing programs and companies' obligations to protect consumer and employee information from these risks[29] and how to properly secure and dispose of information on digital copiers.[30]

III. DATA SECURITY LEGISLATION

The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[31]

---

[27] *See generally* http://www.business.ftc.gov/privacy-and-security/data-security.

[28] *See Mobile App Developers: Start with Security* (Feb. 2013), *available at*http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[29] *See Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

[30] *See Copier Data Security: A Guide for Business* (Nov. 2010), *available at* http://business.ftc.gov/documents/bus43-copier-data-security.

[31] *See, e.g.*, Prepared Statement of the Federal Trade Commission, "Privacy and Data Security: Protecting Consumers in the Modern World," Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacytestimonybrill.pdf; Prepared Statement of the Federal Trade Commission, "Data Security," Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-

Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data. For example, in the case of a breach of Social Security numbers, notifying consumers will enable them to request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. And although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected.

Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA.[32] To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits[33] would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.[34]

---

identity-theft-federal-trade-commission-report/p075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.

[32] The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(*l*).

[33] Non-profits are generally outside the FTC's jurisdiction. 15 U.S.C. §§ 44 & 45(a).

[34] A substantial number of reported breaches have involved non-profit universities and health systems. *See* Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), *available at* http://www.privacyrights.org/data-breach/new.

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology. For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years, a child's Social Security number alone can be combined with another person's information, such as name or date of birth, in order to commit identity theft.[35] Rulemaking authority would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data and we look forward to continuing to work with the Committee and Congress on this critical issue.

[35] FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), *available at* http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft.

William Noonan

Deputy Special Agent in Charge
United States Secret Service
Criminal Investigative Division
Cyber Operations Branch

Prepared Testimony

Before the
United States Senate
Committee on Homeland Security & Governmental Affairs

April 2, 2014

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. Thank you for the opportunity to testify on the risks and challenges the Nation faces from large-scale data breaches of financial information, like those that have been recently reported. The U.S. Secret Service (Secret Service) has decades of experience investigating large-scale criminal cyber intrusions, in addition to other crimes that impact our Nation's financial payment systems. Based on investigative experience and the understanding we have developed regarding transnational organized cyber criminals that are engaged in these data breaches and associated frauds, I hope to provide this committee useful insight into this issue from a federal law enforcement perspective to help inform your deliberations.

The Role of the Secret Service

The Secret Service was founded in 1865 to protect the U.S. financial system from the counterfeiting of our national currency. As the Nation's financial system evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative mission. Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment system by engaging in fraud and other illicit activities. This is not a new trend; criminals have been committing cyber financial crimes since at least 1970.[1]

Congress established 18 USC § 1029-1030 as part of the Comprehensive Crime Control Act of 1984 and explicitly assigned the Secret Service authority to investigate these criminal violations.[2] These statutes first established as specific Federal crimes unauthorized access to computers[3] and the fraudulent use, or trafficking of, access devices[4]—defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other thing of value.[5]

Secret Service investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches, including those of TJ Maxx, Dave & Buster's, Heartland Payment Systems, and others. Over the past four years Secret Service cyber crime investigations have resulted in over 4,900 arrests, associated with approximately $1.37 billion in fraud losses and the prevention of over $11.24 billion in potential fraud losses. Through our work with our partners at the Department of Justice (DOJ), in particular the local U.S. Attorney Offices, the Computer Crimes and Intellectual Property section (CCIPS), the International Organized Crime Intelligence and Operations Center (IOC-2), and others, we are confident we will continue to bring the cyber criminals that perpetrate major data breaches to justice.

---

[1] Beginning in 1970, and over the course of three years, the chief teller at the Park Avenue branch of New York's Union Dime Savings Bank manipulated the account information on the bank's computer system to embezzle over $1.5 million from hundreds of customer accounts. This early example of cyber crime not only illustrates the long history of cyber crime, but the difficulty companies have in identifying and stopping cyber criminals in a timely manner—a trend that continues today.

[2] *See* 18 USC § 1029(d) & 1030(d)(1)

[3] *See* 18 USC § 1030

[4] *See* 18 USC § 1029

[5] *See* 18 USC § 1029(e)(1)

The Transnational Cyber Crime Threat

Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The recently reported data breaches of Target and Neiman Marcus are just the most recent, well-publicized examples of this decade-long trend of major data breaches perpetrated by cyber criminals who are intent on targeting our Nation's retailers and financial payment systems.

The increasing level of collaboration among cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors as they develop expert specialization. These specialties raise both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals. For example, illicit underground cyber crime marketplaces allow criminals to buy, sell and trade malicious software, access to sensitive networks, spamming services, credit, debit and ATM card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users. These digital marketplaces often use various digital currencies, and cyber criminals have made extensive use of digital currencies to pay for criminal goods and services or launder illicit proceeds.

The Secret Service has successfully investigated many underground cyber criminal marketplaces. In one such infiltration, the Secret Service initiated and conducted a three-year investigation that led to the indictment of 11 perpetrators allegedly involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJ Maxx, BJ's Wholesale Club, Office Max, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, these cyber criminals installed "sniffer" programs[6] that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their illegal proceeds by using anonymous Internet-based

[6] Sniffers are programs that detect particular information transiting computer networks, and can be used by criminals to acquire sensitive information from computer systems.

digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.[7]

In data breaches like these the effects of the criminal acts extended well beyond the companies compromised, potentially affecting millions of individual card holders. Proactive and swift law enforcement action protects consumers by preventing and limiting the fraudulent use of payment card data, identity theft, or both. Cyber crime directly impacts the U.S. economy by requiring additional investment in implementing enhanced security measures, inflicting reputational damage on U.S. firms, and direct financial losses from fraud—all costs that are ultimately passed on to consumers.

Secret Service Strategy for Combating this Threat

The Secret Service proactively investigates cyber crime using a variety of investigative means to infiltrate these transnational cyber criminal groups. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify financial institutions and the victim companies with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions, or other third parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cyber crime marketplaces.

A trusted relationship with the victim is essential for confirming the crime, remediating the situation, beginning a criminal investigation, and collecting evidence. The Secret Service's global network of 35 Electronic Crimes Task Forces (ECTF), located within our field offices, are essential for building and maintaining these trusted relationships, along with the Secret Service's commitment to protecting victim privacy.

When the Secret Service identifies a potential network intrusion, the Secret Service contacts the owner of the suspected compromised computer systems in order to assess the data breach and to stop the continued theft of sensitive information and the exploitation of a network. Once the victim of a data breach confirms that unauthorized access to their networks has occurred, the Secret Service works with the local U.S. Attorney's office, or appropriate state and local officials, to begin a criminal investigation of the potential violation of 18 USC § 1030. During the course of this criminal investigation, the Secret Service identifies the malware and means of access used to acquire data from the victim's computer network. In order to enable other companies to mitigate their cyber risk based on current cyber crime methods, we quickly share information concerning the cybersecurity incident with the widest audience possible, while protecting grand jury information, the integrity of ongoing criminal investigations, and the victims' privacy. We share this cybersecurity information through:

[7] Additional information on the criminal use of digital currencies can be referenced in testimony provided by U.S. Secret Service Special Agent in Charge Edward Lowery before the Senate Homeland Security and Governmental Affairs Committee in a hearing titled, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" (November 18, 2013).

- Our Department's National Cybersecurity & Communications Integration Center (NCCIC);
- The Information Sharing and Analysis Centers (ISAC);
- Our ECTFs;
- The publication of joint industry notices;
- Our numerous partnerships developed over the past three decades in investigating cyber crimes; and,
- Contributions to leading industry and academic reports like the Verizon Data Breach Investigations Report, the Trustwave Global Security Report, and the Carnegie Mellon CERT Insider Threat Study.

As we share cybersecurity information discovered in the course of our criminal investigation, we also continue our investigation in order to apprehend and bring to justice those involved. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with law enforcement investigations, occasionally it takes years to finally apprehend the top tier criminals responsible. For example, Dmitriy Smilianets and Vladimir Drinkman were arrested in June 2012, as part of a multi-year investigation Secret Service investigation, while they were traveling in the Netherlands thanks to the assistance of Dutch law enforcement. The alleged total fraud loss from their cyber crimes exceeds $105 million.

As a part of our cyber crime investigations, the Secret Service also targets individuals who operate illicit infrastructure that supports the transnational organized cyber criminal. For example, in May 2013 the Secret Service, as part of a joint investigation through the Global Illicit Financial Team, shut down the digital currency provider Liberty Reserve. Liberty Reserve is alleged to have had more than one million users worldwide and to have laundered more than $6 billion in criminal proceeds. This case is believed to be the largest money laundering case ever prosecuted in the United States and is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and DOJ's Asset Forfeiture and Money Laundering Section. In a coordinated action with the Department of the Treasury, Liberty Reserve was identified as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through our ECTFs, the support provided by our Criminal Investigative Division, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program are all instrumental to the Secret Service's successful network intrusion investigations.

One example of the Secret Service's success in these investigations is the case involving Heartland Payment Systems. As described in the August 2009 indictment, a transnational organized criminal group allegedly used various network intrusion techniques to breach security and navigate the credit card processing environment. Once inside the networks, they installed "sniffer" programs to capture card numbers, as well as password and account information. The

Secret Service investigation, the largest and most complex data breach investigation ever prosecuted in the United States, revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas, search warrants, and Mutual Legal Assistance Treaty (MLAT) requests through our foreign law enforcement partners to identify three main suspects. As a result of the investigation, these primary suspects were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with DOJ's CCIPS, which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[8] The Secret Service's ECTFs are a natural complement to CCIPS, resulting in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions.

The Secret Service also maintains a positive relationship with the DOJ's Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force (NCIJTF), which coordinates, integrates, and shares information related to investigations of national security cyber threats. The Secret Service also often partners with the FBI on various criminal cyber investigations. For example, in August 2010, a joint operation involving the Secret Service, FBI, and the Security Service of Ukraine (SBU), yielded the seizure of 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of 85 terabytes of data, which was eventually transferred to law enforcement authorities in the United States. The data was seized from a criminal Internet service provider located in Odessa, Ukraine, also referred to as a "Bullet Proof Hoster." Thus far, the forensic analysis of these systems has already identified a significant amount of criminal information pertaining to numerous investigations currently underway by both agencies, including malware, criminal chat communications, and PII of U.S. citizens.

The case of Vladislav Horohorin is another example of successful cooperation between the Secret Service and its law enforcement partners around the world. Mr. Horohorin, one of the world's most notorious traffickers of stolen financial information, was arrested on August 25, 2010, pursuant to a U.S. arrest warrant issued by the Secret Service. Mr. Horohorin created the first fully-automated online store which was responsible for selling stolen credit card data. Both CCIPS and the Office of International Affairs at DOJ played critical roles in this apprehension.

[8] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

This case demonstrates the importance of international law enforcement cooperation. Through the Secret Service's 24 international field offices the Service develops close partnerships with numerous foreign law enforcement agencies in order to combat transnational crime. To strengthen our investigations of transnational cyber crime, the Secret Service maintains ECTFs in London and Rome, has assigned agents to INTERPOL and EUROPOL, and operates cyber crime working groups with the Netherlands, Estonia, Lithuania, Latvia, Ukraine, and Germany. The Secret Service also trains numerous international partners on investigating cyber crime; in the past three years the Secret Service has trained over 500 law enforcement officials representing over 90 countries in investigating cyber crimes.

The Secret Service investigations of transnational crime are facilitated by dedicated efforts of the Department of State and the DOJ's Office of International Affairs to establish and execute MLATs, and other forms of international law enforcement cooperation, in addition to the personal relationships that develop between Secret Service agents and their foreign counterparts through these working groups and training efforts. Both the CCIPS and the Office of International Affairs at DOJ played critical roles in the apprehension of Mr. Horohorin. Furthermore, as a result of information sharing, the FBI was able to bring additional charges against Mr. Horohorin for his involvement in a Royal Bank of Scotland network intrusion. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

Within DHS, the Secret Service benefits from a close relationship with Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI). Since 1997, the Secret Service, ICE-HSI, and IRS-CI have jointly trained on computer investigations through the Electronic Crimes Special Agent Program (ECSAP). ICE-HSI is also a member of Secret Service ECTFs, and ICE-HSI and the Secret Service have partnered on numerous cyber crime investigations including the recent take down of the digital currency Liberty Reserve.

To further its cybersecurity information sharing efforts, the Secret Service has strengthened its relationship with the National Protection and Programs Directorate (NPPD), including the NCCIC. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with our Department's NCCIC. The Secret Service continues to build upon its full-time presence at NCCIC to coordinate its cyber programs with other federal agencies.

As a part of these efforts, and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel assigned to the following DHS and non-DHS entities:

- NPPD's National Cybersecurity & Communications Integration Center (NCCIC);
- NPPD's Office of Infrastructure Protection;
- DHS's Science and Technology Directorate (S&T);
- DOJ National Cyber Investigative Joint Task Force (NCIJTF);

- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Office of Terrorist Financing and Financial Crimes (TFFC);
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- DOJ, International Organized Crime and Intelligence Operations Center (IOC-2);
- Drug Enforcement Administration's Special Operations Division;
- EUROPOL; and
- INTERPOL.

The Secret Service is committed to ensuring that all its information sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Secret Service Framework

To protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes.

Electronic Crimes Task Forces

In 1995, the Secret Service New York Field Office established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. In 2001, Congress directed the Secret Service to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."[9]

Secret Service field offices currently operate 35 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes: over 4,000 private sector partners; over 2,500 international, federal, state and local law enforcement partners; and over 350 academic partners. By joining our ECTFs, our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which analyzes evidence collected as a part of Secret Service investigations and disseminates information in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures. CIS also has an operational unit that investigates international cyber-criminals involved in cyber-

[9] *See* Public Law 107-56 Section 105 (appears as note following 18 U.S.C. § 3056).

intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training.

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP): The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI): ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers, or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow for effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF): ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally-focused protective intelligence cases.

These agents are deployed in Secret Service field offices throughout the world and have received extensive training in forensic identification, as well as the preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama, and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and to conduct electronic crimes investigations. Since opening in 2008, the institute has held over 110 cyber and digital forensics courses in 13 separate subjects and trained and equipped more than 2,500 state and

local officials, including more than 1,600 police investigators, 570 prosecutors and 180 judges from all 50 states and three U.S. territories. These NCFI graduates represent more than 1,000 agencies nationwide.

Partnerships with Academia

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT[10] Liaison Program to provide technical support, opportunities for research and development, as well as public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; partner with CERT-SEI and Carnegie Mellon University to support research and development to improve the security of cyberspace and improve the ability of law enforcement to investigate crimes in a digital age; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI to publish the first "Insider Threat Study" examining the illicit cyber activity and insider fraud in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS Science & Technology (S&T), updated the study and released the most recent version just last year, which is published at http://www.cert.org/insider_threat/.

To improve law enforcement's ability to investigate crimes involving mobile devices, the Secret Service opened the Cell Phone Forensic Facility at the University of Tulsa in 2008. This facility has a three-pronged mission: (1) training federal, state and local law enforcement agents in embedded device forensics; (2) developing novel hardware and software solutions for extracting and analyzing digital evidence from embedded devices; and (3) applying the hardware and software solutions to support criminal investigations conducted by the Secret Service and its partner agencies. To date, investigators trained at the Cell Phone Forensic Facility have completed more than 6,500 examinations on cell phone and embedded devices nationwide. Secret Service agents assigned to the Tulsa facility have contributed to over 300 complex cases that have required the development of sophisticated techniques and tools to extract critical evidence.

These collaborations with academia, among others, have produced valuable innovations that have helped strengthen the cyber ecosystem and improved law enforcement's ability to investigate cyber crime. The Secret Service will continue to partner closely with academia and DHS S&T, particularly the Cyber Forensics Working Group, to support research and

[10] CERT—not an acronym—conducts empirical research and analysis to develop and transition socio-technical solutions to combat insider cyber threats.

development of innovate tools and methods to support criminal investigations. **Legislative Action to Combat Data Breaches**

While there is no single solution to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. The Administration previously proposed law enforcement provisions related to computer security through a letter from OMB Director Lew to Congress on May 12, 2011, highlighting the importance of additional tools to combat emerging criminal practices. We continue to support changes like these that will keep up with rapidly-evolving technologies and uses.

Conclusion

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

United States Government Accountability Office
Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, April 2, 2014

INFORMATION SECURITY

Federal Agencies Need to Enhance Responses to Data Breaches

Statement of Gregory C. Wilshusen, Director
Information Security Issues

GAO Highlights

April 2, 2014

INFORMATION SECURITY

Federal Agencies Need to Enhance Responses to Data Breaches

Highlights of GAO-14-487T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

The federal government collects large amounts of PII from the public, including taxpayer data, Social Security information, and patient health information. It is critical that federal agencies ensure that this information is adequately protected from data breaches, and that they respond swiftly and appropriately when breaches occur. Since 1997, GAO has designated information security as a government-wide high-risk area. Further, data breaches at federal agencies have raised concerns about the protection of PII. Federal laws and other guidance specify the responsibilities of agencies in securing their information and information systems and in responding to data breaches.

This testimony addresses federal agencies' efforts to secure their information and respond to data breaches. In preparing this statement, GAO relied primarily on previously published and ongoing work in this area.

What GAO Recommends

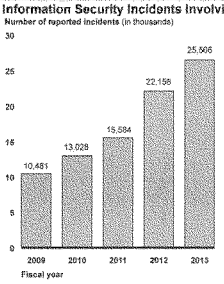
In its December 2013 report, GAO made 22 recommendations to the agencies included in its review aimed at improving their data breach response activities. GAO also recommended that OMB update its guidance on federal agencies' responses to PII-related data breaches. Agency responses to GAO's recommendations varied.

View GAO-14-487T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The number of reported information security incidents involving personally identifiable information (PII) has more than doubled over the last several years (see figure).

Information Security Incidents Involving PII, Fiscal Years 2009 – 2013



Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

As GAO has previously reported, major federal agencies continue to face challenges in fully implementing all components of an agency-wide information security program, which is essential for securing agency systems and the information they contain—including PII. Specifically, agencies have had mixed results in addressing the eight components of an information security program called for by law, and most agencies had weaknesses in implementing specific security controls. GAO and inspectors general have continued to make recommendations to strengthen agency policies and practices.

In December 2013, GAO reported on agencies' responses to PII data breaches and found that they were inconsistent and needed improvement. Although selected agencies had generally developed breach-response policies and procedures, their implementation of key practices called for by Office of Management and Budget (OMB) and National Institute of Standards and Technology guidance was inconsistent. For example,

- only one of seven agencies reviewed had documented both an assigned risk level and how that level was determined for PII data breaches; two agencies documented the number of affected individuals for each incident; and two agencies notified affected individuals for all high-risk breaches.
- the seven agencies did not consistently offer credit monitoring to affected individuals; and
- none of the seven agencies consistently documented lessons learned from their breach responses.

Incomplete guidance from OMB contributed to this inconsistent implementation. For example, OMB's guidance does not make clear how agencies should use risk levels to determine whether affected individuals should be notified. In addition, the nature and timing of reporting requirements may be too stringent.

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee:

Thank you for inviting me to testify today on efforts to protect individuals' personally identifiable information (PII)[1] from data breaches and to notify victims when a data breach has occurred. As you know, in carrying out its responsibilities the federal government collects large quantities of PII, such as taxpayer data, census data, Social Security information, and patient health information, on American citizens and other residents of our nation. Consequently, it is critical that federal agencies take steps to secure the information they collect, retain, and disseminate and that, when events such as data breaches[2] occur, they respond swiftly and appropriately. We first identified the protection of federal information systems as a government-wide high-risk area in 1997 and continued to do so in the most recent update to our high-risk series.[3]

My testimony today will discuss federal agencies' efforts to secure their information—including PII—and systems, and their responses when incidents involving PII occur. In preparing this testimony we relied on previously published work in these areas, as well as the preliminary results from a study whose results will be published later this spring. All the work supporting this statement was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

Background

Data breaches involving PII can occur under many circumstances and for many reasons. They can be inadvertent, such as from the loss of an electronic device, or deliberate, such as from the theft of a device, or a

[1]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[2]The term "data breach" generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information, including PII.

[3]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

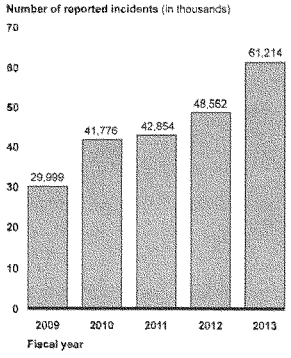
cyber-based attack by a malicious individual or group, foreign nation, terrorist, or other adversary. Incidents have been reported at a wide range of public- and private-sector institutions, including federal, state, and local government agencies; educational institutions; hospitals and other medical facilities; financial institutions; information resellers; retailers; and other types of businesses.

The loss or unauthorized disclosure or alteration of the information residing on federal systems, which can include PII, can lead to serious consequences and substantial harm to individuals and the nation. Thus it is critical that federal agencies protect their systems and the information on them and respond to data breaches and cyber incidents when they occur.

Information Security Incidents Have Increased

Over the last several years, federal agencies have reported an increasing number of information security incidents to the U.S. Computer Emergency Readiness Team (US-CERT). These include both cyber- and non-cyber-related incidents, and many of them involved PII. Figure 1 shows that the total number of security incidents reported annually more than doubled from fiscal year 2009 to fiscal year 2013.

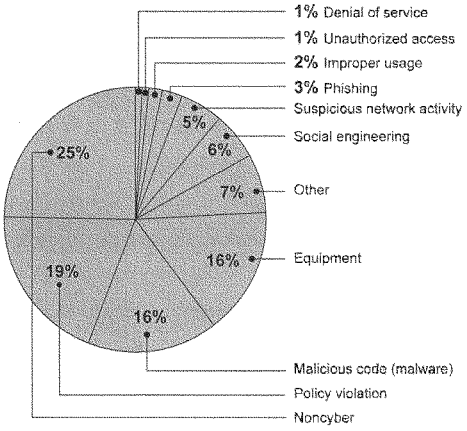
Figure 1: Information Security Incidents Reported to US-CERT by All Federal Agencies, Fiscal Years 2009 – 2013



Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

These incidents are categorized by type. Figure 2 shows the categories into which incidents reported in fiscal year 2013 fell.

Figure 2: Information Security Incidents by Category, Fiscal Year 2013

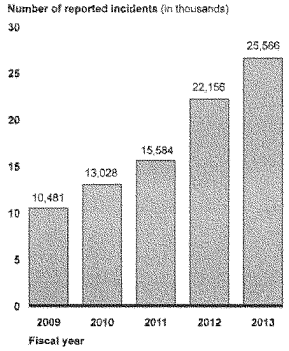


Source: GAO analysis of US-CERT data for fiscal year 2013.

Moreover, a significant number of security incidents reported by agencies have involved PII.[4] Figure 3 shows that the number of incidents involving PII for fiscal years 2009 through 2013 increased over 140 percent.

[4]PII-related incidents can include both cyber- and non-cyber-related incidents.

Figure 3: Incidents Involving PII, Fiscal Years 2009 – 2013



Source: GAO analysis of US-CERT data for fiscal years 2009-2013.

Data breaches at federal agencies have received considerable publicity and raised concerns about the protection of PII at those agencies. Most notably, in May 2006, the Department of Veterans Affairs (VA) reported that computer equipment containing PII on about 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. More recent examples of incidents that compromised individuals' personal information further highlight the impact that such incidents can have:

- In July 2013, hackers stole a variety of PII on more than 104,000 individuals from a Department of Energy system. Types of data stolen included Social Security numbers, birth dates and locations, bank account numbers and security questions and answers. According to the department's Inspector General, the combined costs of assisting affected individuals and lost productivity—due to federal employees being granted administrative leave to correct issues stemming from the breach—could be more than $3.7 million.[5]
- In May 2012, the Federal Retirement Thrift Investment Board (FRTIB) reported a sophisticated cyber attack on the computer of a contractor

[5]Department of Energy, Office of the Inspector General, *The Department of Energy's July 2013 Cyber Security Breach*, DOE/IG-0900 (Washington, D.C.: Dec. 6, 2013).

that provided services to the Thrift Savings Plan. As a result of the attack, PII associated with approximately 123,000 plan participants was accessed. According to FRTIB, the information included 43,587 individuals' names, addresses, and Social Security numbers, and 79,614 individuals' Social Security numbers and other PII-related information.

- In March 2012, a laptop computer containing sensitive PII was stolen from a National Aeronautics and Space Administration employee at the Kennedy Space Center. As a result, 2,300 employees' names, Social Security numbers, dates of birth, and other personal information were exposed.
- In February 2009, the Federal Aviation Administration notified employees that an agency computer had been illegally accessed and that employee PII had been stolen electronically. Two of the 48 files on the breached computer server contained personal information about more than 45,000 agency employees and retirees.

Federal Laws and Policies Establish Agency Information Security Responsibilities

Title III of the E-Government Act of 2002, known as the Federal Information Security Management Act (FISMA), establishes a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible for, among other things, providing information security protections commensurate with the risk and magnitude resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor or other organization on behalf of an agency. These protections are to provide federal information and systems with integrity—preventing improper modification or destruction of information; confidentiality—preserving authorized restrictions on access and disclosure; and availability—ensuring timely and reliable access to and use of information.

Under FISMA, agencies are required to develop procedures for detecting, reporting, and responding to security incidents, consistent with federal standards and guidelines, including mitigating risks associated with such incidents before substantial damage is done. The law also requires the operation of a central federal information security incident center that compiles and analyzes information about incidents that threaten information security. The Department of Homeland Security (DHS) was given the role of operating this center, which became US-CERT, by the

Homeland Security Act. DHS's role is further defined by Office of Management and Budget (OMB) guidance, which requires that incidents involving PII be reported to US-CERT within 1 hour of discovery. US-CERT is also responsible for providing timely technical assistance to operators of agency information systems regarding security incidents, including offering guidance on detecting and handling incidents.

In addition to establishing responsibilities for agencies, FISMA assigns specific responsibilities to OMB, the National Institute of Standards and Technology (NIST) and inspectors general:

- OMB is to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies (except with regard to national security systems). It is also responsible for reviewing, at least annually, and approving or disapproving agency information security programs.
- NIST's responsibilities include developing security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of risk levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.
- Agency inspectors general are required to annually evaluate the information security program and practices of their agency. The results of these evaluations are to be submitted to OMB, and OMB is to summarize the results in its reporting to Congress.

In July 2010, the Director of OMB and the White House Cybersecurity Coordinator issued a joint memorandum stating that DHS was to exercise primary responsibility within the executive branch for the operational aspects of cybersecurity for federal information systems that fall within the scope of FISMA.

Agencies Continue to Face Challenges in Effectively Securing Their Information

In September 2013 we issued the most recent of our periodic reports on federal agencies' compliance with the requirements of FISMA.[6]

[6]GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, GAO-13-776 (Washington, D.C.: Sept. 26, 2013).

Specifically, we reported that, for fiscal year 2012, 24 major federal departments and agencies covered by the Chief Financial Officers Act[7] had established many of the components of an agency-wide information security program, as required by FISMA, but had only partially established others.

In particular, with regard to the eight components of an agency-wide security program,

- 18 agencies had fully implemented a program for managing information security risk, and 6 had partially implemented such a program;
- 10 agencies had fully documented security policies and procedures, while 12 had partially documented them;[8]
- 18 agencies had selected security controls for their systems, but 6 had only partially implemented this practice;
- 22 agencies had established a security training program, and 2 had partially established such a program;
- 13 agencies were monitoring security controls on an ongoing basis, but 10 agencies had not fully implemented a continuous monitoring program;[9]
- 19 agencies had established a program for remediating weaknesses in their security policies, practices, and procedures, while 5 had not fully implemented elements of a remediation program;
- 20 agencies had established an incident response and reporting program, but 3 agencies had not fully established such a program;[10] and
- 18 agencies had fully established a program for ensuring continuity of operations in the event of a disruption or disaster, but 5 agencies partially implemented a continuity of operations program.[11]

[7]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[8]An additional 2 agencies did not fully evaluate this program component in 2012.

[9]One additional agency did not fully evaluate this program component in fiscal year 2012.

[10]One additional agency did not fully evaluate this program component in fiscal year 2012.

The extent to which the agencies had implemented security program components showed mixed progress from fiscal year 2011 to fiscal year 2012. For example, according to inspectors general reports, the number of agencies that had analyzed, validated, and documented security incidents increased from 16 to 19, while the number able to track identified weaknesses had declined from 20 to 15.

In addition, although most agencies had implemented elements of their security programs, we and inspectors general continued to identify weaknesses in elements of their programs, such as the implementation of specific security controls. Specifically, most major federal agencies had weaknesses in major categories of information security controls, as defined by our *Federal Information System Controls Audit Manual*.[12]

Table 1 shows, for fiscal year 2012, the number of the 24 major federal agencies that had weaknesses in the five major control categories.

Table 1: Information Security Control Weaknesses at 24 Major Agencies in Fiscal Year 2012

Control category	Number of agencies with weaknesses
Security management	24
Access controls	23
Configuration management	24
Segregation of duties	18
Contingency planning	24

Source: GAO analysis of agency inspector general data.

Note: *Security management* includes an agency-wide information security program to provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; *access controls* ensure that only authorized individuals can read, alter, or delete data; *configuration management* controls provide assurance that only authorized software programs are implemented; *segregation of duties* reduces the risk that one individual can independently perform inappropriate actions without detection; and *contingency planning* includes continuity of operations, which provides for the prevention of significant disruptions of computer-dependent operations.

Illustrating the extent to which weaknesses continue to affect the 24 major federal agencies, in fiscal year 2013, inspectors general at 21 of the 24 agencies cited information security as a major management challenge for their agency, and 18 agencies reported that information security control

[11]One additional agency did not fully evaluate this program component in fiscal year 2012.

[12]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

deficiencies were either a material weakness or significant deficiency[13] in internal controls over financial reporting in fiscal year 2013. These weaknesses show that information security continues to be a major challenge for federal agencies, putting federal systems and the information they contain, including PII, at increased risk. We and agency inspectors general have continued to make numerous recommendations to agencies aimed at improving their information security posture. Fully implementing these recommendations will strengthen agencies' ability to ensure that their information, including PII, is adequately protected.

Agencies Need to Improve Responses to Data Breaches and Cyber Incidents

Even when information security programs have been implemented effectively, data breaches can occur. Accordingly, OMB and NIST have specified key practices for responding to PII data breaches.[14] These include *management practices* such as establishing a data breach response team and training employees on roles and responsibilities for breach response, and *operational practices*, such as preparing reports on suspected data breaches and submitting them to appropriate internal and external entities, assessing the likely risk of harm and level of impact of a suspected breach, offering assistance to affected individuals (if appropriate), and analyzing the agency's breach response and identifying lessons learned. Table 2 provides more details on these key management and operational practices.

[13]A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[14]These practices were specified in guidance documents issued by OMB and NIST. See OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (Washington, D.C.: May 22, 2007); and NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

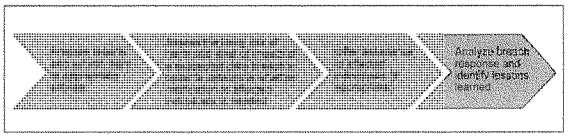
Table 2: Key Management and Operational Practices to Be Included in Policies for Responding to Data Breaches Involving Personally Identifiable Information (PII)

Key management practice	Description
Establish a data breach response team	While technical remediation is usually handled by IT security staff, agencies should create a team to oversee responses to a suspected or confirmed data breach, including the program manager of the program experiencing the breach, chief information officer, chief privacy officer or senior agency official for privacy, communications office, legislative affairs office, general counsel, and the management office which includes budget and procurement functions.
Train employees on roles and responsibilities for breach response	Agencies should train employees on their data breach response plan and their roles and responsibilities should a breach occur. Specifically, OMB requires agencies to initially train employees on their privacy and security responsibilities before permitting access to agency information and information systems and thereafter provide at least annual refresher training to ensure employees continue to understand their responsibilities.
Key operational practice	**Description**
Prepare reports on suspected data breaches and submit them to appropriate internal and external entities	Agencies should establish procedures for promptly reporting a suspected or confirmed breach to the appropriate internal management entities and external oversight entities. For example, the breach response team should be notified about all suspected or confirmed breaches. Further, agencies must report all incidents involving PII to US-CERT within 1 hour of discovering the suspected or confirmed incident.
Assess the likely risk of harm and level of impact of a suspected data breach in order to determine whether notification to affected individuals is needed	In addition to any immediate remedial actions they may take, agencies should assess a suspected or confirmed breach to determine if there is a likely risk of harm and the level of impact, if applicable. OMB outlined five factors that should be considered in assessing the likely risk of harm: (1) nature of the data elements breached (2) number of individuals affected (3) likelihood the information is accessible and usable (4) likelihood the breach may lead to harm and (5) ability of the agency to mitigate the risk of harm. Once a risk level is determined, agencies should use this information to determine whether notification to affected individuals is needed and, if so, what methods should be used. OMB instructed agencies to be mindful that notification when there is little or no risk of harm might create unnecessary concern and confusion. It also stated that while the magnitude of the number of affected individuals may dictate the method chosen for providing notification, it should not be the determining factor for whether an agency should provide notification.
Offer assistance to affected individuals (if appropriate)	Agencies should have procedures in place to determine whether services such as credit monitoring should be offered to affected individuals to mitigate the likely risk of harm. OMB instructed agencies that, while assessing the level of risk in a given situation, they should simultaneously consider options for attenuating that risk.
Analyze breach response and identify lessons learned	Agencies should review and evaluate their responses to a data breach, including any remedial actions that were taken, and identify lessons learned, which should be incorporated into agency security and privacy policies and practices as necessary. NIST recommended holding a "lessons learned" meeting with all involved parties after a major incident and periodically after lesser incidents, as resources permit, to assist in handling similar incidents and improving security measures.

Source: GAO analysis of OMB and NIST guidance.

In December 2013, we reported on our review of issues related to PII data breaches.[15] The eight agencies in our review[16] had generally developed, but inconsistently implemented, policies and procedures for responding to a data breach involving PII that addressed key practices. Specifically, with few exceptions, the agencies reviewed addressed the key management and operational practices in their policies and procedures. However, they did not consistently implement the operational practices, as summarized in figure 4.

Figure 4: Operational Steps in Data Breach Response Practices



Source: GAO analysis of OMB and NIST guidelines.

For example,

- Of the seven agencies[17] we reviewed, only the Internal Revenue Service (IRS) consistently documented both an assigned risk level and how that level was determined for PII-related data breach incidents; only the Army and IRS documented the number of affected individuals for each incident; and only the Army and the Securities and Exchange Commission notified affected individuals for all high-risk breaches.
- The seven agencies did not consistently offer credit monitoring to individuals affected by PII-related breaches.
- None of the seven agencies consistently documented lessons learned from PII breaches, including corrective actions to prevent similar

[15]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[16]These agencies were the Centers for Medicare & Medicaid Services, Department of the Army, Department of Veterans Affairs, Federal Deposit Insurance Corporation, Federal Reserve Board, Federal Retirement Thrift Investment Board, Internal Revenue Service, and Securities and Exchange Commission.

[17]We did not include FRTIB in our analysis of agency implementation of key operational practices because it reported experiencing only one incident involving PII in fiscal year 2012.

incidents in the future or whether better security controls could help detect, analyze, and mitigate future incidents.

Incomplete guidance from OMB contributed to this inconsistent implementation. For example, OMB's guidance does not make clear how agencies should use risk levels in making a determination about notification to affected individuals. Further, OMB guidance states that the risk levels should help determine when and how notification should be provided, but it does not set specific requirements for notification based on agency risk determinations.

In addition, OMB guidance for reporting on data breaches involving PII may be too stringent. Specifically, OMB guidance requires that DHS collect information about PII-related breaches within 1 hour, but officials at US-CERT and the agencies in our review generally agreed that this requirement was difficult to meet and may not provide US-CERT with the best information. For example, some agencies noted that it is difficult to provide a meaningful report on a breach within 1 hour since relevant information—such as how much PII was affected or the extent of the risk—may not be available within that time frame.

Agency officials also questioned the value of reporting certain types of PII breaches, such as paper-based incidents or incidents involving the loss of hardware containing encrypted PII, individually to US-CERT, as currently required. Officials from US-CERT agreed that their office should not be receiving all PII-related incident reports individually as they occur.

According to DHS officials, the PII-related incident data they collect are not generally used to help remediate incidents or provide technical assistance to agencies. Rather, the information is compiled in accordance with certain FISMA requirements and reported to OMB. We determined that the limited use of these data calls into question OMB's requirement that such incidents be reported within 1 hour. US-CERT officials also noted that the vast majority of PII-related data breaches are not cybersecurity related—that is, they do not involve attacks on or threats to government systems or networks. Thus receiving information about such incidents on an individual basis may not be useful to the office in pursuing its mission.

Finally, we reported that seven of the eight agencies in our review had not requested technical assistance from US-CERT when PII data breaches have occurred. DHS officials said that US-CERT is not equipped to assist agencies in remediating paper-based incidents, and agencies agreed that issues they encounter in dealing with PII breaches are generally best addressed by agency general counsel staff or privacy officers. DHS's

Privacy Office has developed guidance that addresses agencies' obligations to protect PII and procedures to follow when a suspected PII incident occurs, but this is geared more toward developing agency response capabilities in general rather than supporting decision-making related to specific incidents.

In our report, we recommended that OMB revise its guidance on federal agencies' response to PII-related data breaches to include (1) guidance on notifying affected individuals based on a determination of the level of risk; (2) criteria for determining whether to offer assistance, such as credit monitoring, to affected individuals; and (3) revised requirements for reporting PII-related breaches to US-CERT. In commenting on our draft report, officials from OMB's Office of Information and Regulatory Affairs stated that our recommendation did not sufficiently specify what supplemental guidance was needed; we subsequently revised the draft recommendation to provide greater specificity.

We also made a number of recommendations to the individual agencies in our review to improve their response to data breaches involving PII. Specifically, we recommended, among other things, that several of the agencies (1) consistently document risk levels and how those levels are determined for PII-related data breach incidents; (2) document the number of affected individuals for each incident; and (3) identify lessons learned from responses to PII breaches. Agencies varied in the extent to which they concurred with these recommendations, with some providing information pertaining to the recommendations. In response to agencies' comments, we clarified or deleted three draft recommendations but retained the rest as still warranted.

Agencies Need to Improve Cyber Incident Response Practices

In a forthcoming report, to be issued later this spring, we plan to provide the results of our study of federal agencies' ability to respond to cyber incidents.[18] More specifically, we have determined the extent to which (1) federal agencies are effectively responding to cyber incidents, and (2) DHS is providing cybersecurity incident assistance to agencies.

While these results are still subject to revision, we estimate, based on a statistical sample of cyber incidents reported in fiscal year 2012, that the 24 major federal agencies did not effectively or consistently demonstrate actions taken in response to a detected cyber incident in about 65 percent

[18]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (forthcoming).

of reported incidents.[19] For example, agencies identified the scope of incidents in the majority of cases, but did not always demonstrate that they had determined the impact of an incident. In addition, agencies did not consistently demonstrate how they had handled other key activities, such as whether actions to prevent the recurrence of an incident were taken.

We also reviewed six selected agencies in greater depth and found that, while they had developed parts of policies, plans, and procedures to guide incident response activities, their efforts were not comprehensive or fully consistent with federal requirements. The inconsistencies in agencies' incident response activities suggest that additional oversight, such as that provided by OMB and DHS during the CyberStat review process,[20] may be warranted. However, these meetings generally have not covered agencies' incident response practices.

With regard to DHS's role, we observed that DHS provides various services to agencies to assist them in preparing to handle incidents, maintain awareness of the current threat environment, and deal with ongoing incidents addressing cyber incidents. However, opportunities exist to enhance the usefulness of these services, such as improving reporting requirements and evaluating the effectiveness of these services.

To improve the effectiveness of government-wide cyber incident response activities, we are planning to make recommendations to OMB and DHS to address agency response practices. We also plan to make recommendations to the six selected agencies in our review to improve their cyber incident response programs.

In summary, the increasing number of cyber incidents at federal agencies, many involving the compromise of PII, highlights the need for focused agency action to ensure the security of the large amount of sensitive personal information collected by the federal government. These actions include establishing comprehensive agency-wide information security programs and consistently and effectively responding to incidents

[19]There is 95 percent confidence that the estimate falls between 58 and 72 percent.

[20]CyberStat reviews are in-depth sessions with National Security Staff, OMB, DHS, and an agency to discuss that agency's cybersecurity posture and opportunities for collaboration.

when they occur. As we and inspectors general have long pointed out, federal agencies continue to face challenges in effectively implementing all elements of their information security programs. Likewise, agencies have not been consistent or fully effective in responding to data breaches and cyber incidents. Ongoing improvements in these areas are needed to help ensure that the personal information entrusted to the government by American citizens and other individuals will be protected.

Chairman Carper, Ranking Member Dr. Coburn, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include John A. de Ferrari and Jeffrey Knott (assistant directors), Larry E. Crosland, Marisol Cruz, and Lee McCracken.

TESTIMONY OF TIM PAWLENTY

Chief Executive Officer, The Financial Services Roundtable

Committee on Homeland Security and Government Affairs

Hearing entitled

"Data Breach on the Rise: Protecting Personal Information from Harm"

April 2, 2014

342 Dirksen Senate Office Building

Chairman Carper, Ranking Member Coburn, Members of the Committee, thank you for this opportunity to appear before you today to address the important topic of data breaches and the further steps needed to better protect personal information and the payment system from cyber threats.

The Financial Services Roundtable (FSR) is a trade association representing the full range of the country's largest financial service companies. Our members include leading banking, insurance, asset management, finance and payment companies.

Cyber security has been a key focus area for FSR and our companies for decades. Since 1996, "BITS" -- the technology policy division of FSR, has played an important leadership role in cyber security, fraud reduction, vendor management, payments and emerging technologies.

Cyber risk is increasing in pace, complexity and potential impact. The threat has expanded from fraudsters committing financial theft to *hacktivists* causing disruptions and nation states threatening serious data manipulation and destruction. Cyber risk affects all institutions in our sector – large and small, banks, credit unions, insurers and investment firms.

Like everyone here, we were dismayed by the scale and scope of the recent data breaches at respected merchants and retailers. It is an indication of how cyber threats have intensified in recent years. It also represents an important opportunity for the financial services sector to partner with the merchant and retailer sector to mitigate cybersecurity threats and better protect customers in the broader payments ecosystems.

A recent *Washington Post* report suggested that over 3,000 companies were alerted to data breaches by federal agents in 2013. Even more disturbing, most of the companies did not even know they were breached. And this number only represents the number of cases in which federal agents were aware an attack occurred. A recent National Intelligence Assessment, cited by the *Washington Post*, concluded massive cyber-attack campaigns are ongoing and mostly generated from abroad.

The financial services sector is better prepared than other sectors to defend against and respond to cyber attacks. Individual financial institutions have and continue to invest substantial resources in personnel, products and services to defend themselves. We have one of the strongest private information sharing process of any critical infrastructure sector through our Financial Sector Information Sharing and Analysis Center (FS-ISAC), and we have been active supporters of our sector coordinating council – the Financial Services Sector Coordinating Council. Industry-wide initiatives are under way to identify and take action on information sharing, tactical operations, and investments in research and development. We plan and run simulations to improve our defenses and resiliency.

Financial institutions are also regulated and are examined to ensure compliance with comprehensive data security, privacy protection, vendor management and resiliency requirements. Over the past 15 months, the financial services sector has worked closely with the Treasury Department, regulators and other government agencies to improve cyber defenses. One example of these efforts is our involvement in the development of a cybersecurity framework for

critical infrastructure entities outlined in the President's Executive Order and Policy Directive on cyber security released in February 2013.

But we live in a networked world where the payment system is interconnected and all parts of the chain must have robust cybersecurity.

The implications of recent data breaches are profound, and they raise questions about cyber responsibility, new technologies, relationship between retailers and credit card companies (issuers and networks), technology standards, and many other issues.

These issues are incredibly important to FSR members and Sandy's members as well. So, about a month and a half ago, our teams got together to chart a course for working together to tackle these issues.

We established the Merchant and Financial Services Cybersecurity Partnership. The Partnership's mission is to work collaboratively across the payments system to enhance security to better protect customers and their data from cyber threats. Our goals include improving overall security across the payments ecosystem and to bolster consumer confidence in the security of their payment data and the systems used to process payments.

On February 27, Sandy and I convened the first meeting of the Partnership's Advisory Council which consists of 18 CEOs of major financial services and merchants/retailers trade associations. We decided to focus on five key areas and we then reached-out to executives from our member companies to serve on five working groups. We have strong participation from all key sectors of our industries and our working groups will begin their work shortly. Our five working groups are focused on the following topics:

- Threat information sharing,
- Cybersecurity risk mitigation,
- Advanced card present security technology,
- Card not present and mobile security, and
- Cybersecurity and data breach notification.

I would like to briefly discuss each of these areas.

Threat Information Sharing

The Threat Information Sharing working group will focus upon the capacity to share information regarding cyber threats and vulnerabilities within and between the retail and financial services industries. Both the retail and financial services industries must facilitate analysis and share threat information that identifies potentially fraudulent activities in its earliest stages. Doing so will bolster our ability to identify, thwart, and defend against attacks.

To accomplish this objective, we will explore options for inter-industry threat information sharing. This may include coordination with National Cyber Forensics Training Alliance (NCFTA), the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other information sharing models and prospective partnerships. Existing information sharing avenues must be fully leveraged by both the financial services sector and retailers. We must also identify additional ways to facilitate threat information between the private and public sector.

Cybersecurity Risk Mitigation

The Cybersecurity Risk Mitigation Working Group will facilitate discussions with key stakeholders in the retail and financial services space on cyber risk mitigation and explore new technologies that allow us to better protect consumers.

Many of our member companies have effective technologies and practices in place to mitigate cyber risk. Although we must always be developing better technology and practices, progress can also be made by having industry leaders share best practice information with industry colleagues. This is especially important for smaller institutions that may not have the experience or resources to easily develop robust cyber security techniques.

Advanced Card Present Security Technology

The Advanced Card Present Security Technology Working Group will identify areas to improve technology in the card present payments ecosystem. We seek to enhance and better protect the security of the data, and to render any stolen data useless.

The specifics are still being developed, but some areas under consideration include: end-to-end data encryption; tokenization; a roadmap to move beyond the magnetic stripe; and innovative technologies.

Card Not Present and Mobile Security

The *Card Not Present and Mobile Security* working group will develop methods to enhance payment security in the mobile or card-not-present environments. E-commerce and other technology innovations increase the frequency of transactions that happen without the card present. We must understand that our obligation to protect consumer data must faetor into this new reality and identify ways to bolster our defenses.

Similar to the previous working group, the specifics are being developed but elements under consideration include: end-to-end data encryption; tokenization; customer identification improvements; and the ability to leverage new, more secure next generation top level domain environments to be launched by the financial services industry.

Cybersecurity & Data Breach Notification

The Cybersecurity and Data Breach Notification working group will identify the appropriate legislative policy to ensure the private sector takes actions necessary to notify and protect consumers if a breach occurs.

The group is considering whether there should be a federal standard for breach notification, steps to better coordinate with law enforcement agencies, as well as additional tools legislators could authorize to enhance cyber security and better protect consumers.

While we will continue to pursue industry solutions to better protect consumers, there is an important need for Congressional action.

Congressional Action

The question before the Committee today is what government can and should do to bolster the private sector and increase our ability to protect consumers. As a partnership, we are considering that very same question.

Senators Carper and Blunt have introduced S. 1927, the "Data Security Act of 2014." Their legislation preempts state law on issues related to data security, investigation, and notice. The legislation establishes a notification standard that is based on "substantial harm or inconvenience." And, financial institutions that comply with Graham-Leach-Bliley Act standards would be deemed in compliance on notification requirements.

I cannot speak on behalf of the partnership because we are still developing our views, but I can say that the Financial Services Roundtable appreciates the legislation and looks forward to working with the Senators and this Committee to achieve its objectives.

But more important than breach notification requirements are the efforts to prevent data breaches in the first place. To that end, FSR and many others have focused on effective cyber threat information sharing. Institutions must have the necessary liability protections to share threat information with private partners and the government. Further, those liability protections should extend to good faith actions taken to defend data, the financial system, and consumers.

We cannot overstate the importance to our industries and our customers of passing this legislation. Having the freedom to share information will give us an improved ability to stop attacks in real time and prevent attacks from occurring in the first place. While we understand and respect privacy concerns, the benefits from this legislation far outweigh potential downsides. FSR supported the *Cyber Intelligence Sharing and Protection Act of 2013*, commonly known as CISPA passed by the House. We understand that the Senate Intelligence Committee is actively working on cyber threat information legislation and we strongly and urgently encourage those efforts.

While the financial services sector continues to improve information sharing communications, the progress will likely remain inadequate without congressional actions to enhance, facilitate, and protect threat information sharing across sectors and with government. Information sharing

legislation would further strengthen the ability of the private sector and the federal government to work together to develop a more effective information sharing framework.

Conclusion

Rather than retreating to our respective silos, the retail and financial services sectors have decided to work together to benefit our customers and the economy. Increased cyber security may lead to some short-term cost increases and inconveniences, but it is an investment well worth making. We believe the partnership between the financial services and retail industries will be very helpful. We will keep you informed of our efforts and appreciate the Congress' level-headed examination of cyber threats to our economy. We also hope you will pass the legislation we referenced here today. It is overdue and urgently needed.

Thank you for the opportunity to appear before this Committee. I look forward to continuing to work with you to address cyber-security, data breaches and many other issues. I would be happy to address any questions the Committee may have.

TESTIMONY OF SANDRA L. KENNEDY

PRESIDENT,
RETAIL INDUSTRY LEADERS ASSOCIATION

BEFORE THE

SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITEE

HEARING ON

"DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM"

APRIL 2, 2014

Chairman Carper, Ranking Member Coburn and members of the Committee, my name is Sandra Kennedy and I am the President of the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about the cybersecurity threats we collectively face and the steps that the retail industry is taking to address them and protect consumers. I am particularly pleased to be testifying alongside Governor Tim Pawlenty, CEO of the Financial Services Roundtable, to share details about a unique inter-industry partnership aimed at strengthening protections for consumers.

RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together are responsible for more than $1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

The threat of cyber attacks is understood now to be all too common. While retailers place extremely high priority on data security, cyber-criminals are persistent and their methods of attack are increasingly sophisticated. As we have seen, no organization, be it business, education or government, is immune from attacks. Recent reports that federal agents in the last year alone notified more than 3,000 businesses of breaches to their systems offer a sense of the scale of the threat and the persistence of the criminals.

I. Defending Against Cyber Attacks

Retailers take the threat of cyber attacks very seriously, investing tremendous resources in talent and technology to defend against them. But as experts testifying before this Committee have noted, while security measures help thwart attacks, no system is invulnerable. Retailers understand that defense against cyber attacks must be an ongoing effort, evolving to address the changing nature of the threat. To that end, in January RILA launched a comprehensive Cybersecurity and Data Privacy Initiative. The initiative is designed to enhance the industry's existing cybersecurity and privacy efforts, inform the public dialogue, and build and maintain consumer trust.

RILA's initiative addresses three areas: overall Cybersercurity; enhanced Payment Systems Security; and Consumer Privacy. I will describe each in turn.

A. Cybersecurity:

Formation of a Retail Cybersecurity Leaders Council – Retailers rebuff cyber attacks every day and the resulting lessons learned can, if shared, strengthen protections across the entire industry. The Retail Cybersecurity Leaders Council, which is made up of senior retail executives responsible for cybersecurity, is working to improve industry-wide cybersecurity by sharing threat information and discussing effective security solutions in a trusted forum.

Federal Data Breach Notification Legislation – RILA has engaged with lawmakers to promote federal data security breach notification legislation that sets a national baseline.

Federal Cybersecurity Legislation – RILA has committed to engage with policymakers to help develop federal cybersecurity legislation focused on enabling measures widely viewed as being effective to strengthen cybersecurity such as appropriate information-sharing and R&D investments.

B. Improved Payments Security:

Eliminate the Mag-Stripe: The existing magnetic stripe technology used on credit and debit cards issued in the United States is antiquated and vulnerable. RILA is advocating that it be phased out in favor of more secure technology widely used in other parts of the world.

Universal PIN Security and Chip-based Smart Card Technology - RILA will continue to press the card networks and the issuing banks to migrate to universal PIN security and chip-based smart card technology. In the event of a successful cybersecurity breach, the dynamic security features of such technology renders stolen card data largely useless.

System-Wide Collaboration - Enhanced card security is an important first step, but innovation in the payments security must outpace criminal threats. Therefore, RILA has committed to forge a partnership with the other members of the payments ecosystem to collaborate on long-term, comprehensive approaches to address evolving threats.

C. Consumer Privacy:

RILA's cybersecurity and payments security efforts will go a long way to help address consumer privacy expectations, as consumers want and expect data about them to which retailers have access to be protected. Consumers also welcome tailored services, yet may have questions about the data practices required to provide them. RILA has convened a forum in which retailers can develop and share data and privacy insights and best practices, and where useful we will help to shape and then promote data practices that are consistent with RILA's privacy principles.

In the months since its launch, the initiative has made progress on multiple fronts.

The Retail Cybersecurity Leaders Council (Council) has begun work to establish a mechanism for improved industry-wide threat information sharing. A recent survey of the group found that a majority of RILA members already participated in informal or non-retail specific threat information sharing, but that

expanding such efforts to include engagement with other partners and government would bolster efforts to defend against the growing threat. This group has already made considerable progress toward establishing a trusted forum through which threat information can be better shared among trusted parties.

Specifically, through the Council, RILA recently formed a partnership with the National Cyber-Forensics and Training Alliance (NCFTA), a respected non-profit organization specializing in establishing public-private partnerships. The NCFTA partnership will provide retailers with an established and trusted forum where retailers can collaborate with a diverse set of businesses and government agencies on effective solutions to combat cyber-criminals.

Just last week, the Council convened over twenty-five retail executives from some of America's largest retailers for a two-day conference at the NCFTA facilities in Pittsburgh, PA. The group explored various information-sharing models and governance structures, and met with experts from government, law enforcement, academia, and solution providers to gain further insight on the cyber threat landscape and leading practices in cybersecurity. This meeting was very productive and there was broad consensus in the group in support of continued collaboration and information sharing.

II. Data Breach Notification

When attacks are successful and compromise customer data, retailers believe that their customers have the right to be notified as promptly as possible. Retailers also believe that they have an obligation to provide customers whose personal information has been compromised with information that is as accurate and actionable as possible so that they can take steps to protect themselves. In order to notify customers as quickly as possible, in RILA's experience retailers typically conduct their response in parallel tracks – while one group investigates the attack to determine if there was unauthorized access to or acquisition of personal information, a second group begins preparing to distribute notifications as necessary to affected customers.

Where feasible, retailers provide direct notification, such as written notification by mail, email or phone. Merchants also may alert customers through alternative means such as website postings or the media.

To improve upon current processes, RILA supports federal data breach notification legislation that is practical, proportional and sets a single national standard that replaces the patchwork of state laws in place today. A federal standard will help ensure that customers receive timely and accurate information following a breach. Any legislation considered by Congress should include three essential provisions. First, legislation should include strong state preemption language that would create a single national standard. Second, legislation should consider the practical realties following a breach. Specifically, adequate time must be allowed prior to a mandated notification in order to allow organizations to secure the breached environment, conduct a thorough forensics investigation and then, based off this assessment, determine who may have been affected by the cyber attack and what information was compromised. Furthermore, reasonable delays in notification should be allowed if requested by law enforcement for investigative purposes or national security reasons. Third, notification requirements should be linked to risk of harm, for example considering whether or not the compromised information is in a form usable to commit financial fraud or identify theft.

III. Legislative Proposals

As you know, there have been multiple bills introduced in both the Senate and House of Representatives in relation to data breach notification, including one by Chairman Carper. As mentioned, we believe that it is imperative that strong state preemption and proportional risk of harm be a part of any legislation and we applaud Senator Carper for including such provisions in S. 1927. Other legislative solutions also include provisions that retailers support and as the bills move through the legislative process, RILA looks forward to working with Congress on enacting legislation that provides customers with concise, accurate and timely notification.

IV. Partnership between Merchants and Financial Services

While there is much that retailers can undertake as an industry, retailers recognize that much more can be done by collaborating with other stakeholders as well. Cyber criminals who attack retailers do so in hopes of accessing sensitive consumer financial information, specifically credit and debit card information. Retailers believe that a strong defense against cyber attacks requires not only that retailers stay ahead of the threats they face, but also that payments technology and process advance such that any stolen data cannot be used to counterfeit cards and commit fraud. For example, retailers believe that enhanced technology widely available elsewhere in the world known as Chip and PIN would render stolen data largely valueless to cyber criminals.

The interconnectedness of merchant and financial services industries, and the common obligation to protect our shared customers, is such that collaboration among the two industries is essential. To that end, in February, RILA joined with the Financial Services Roundtable and 16 other associations representing merchants and financial institutions of all types and sizes to establish Merchant – Financial Services Cybersecurity Partnership, a group that is dedicated to strengthening overall security across the payments ecosystem and bolstering consumer confidence in the payments system.

The historical tension between these two industries is well chronicled. And while we expect that there will continue to be issues on which we disagree, the common threat that we face is such that we have an obligation to consumers to find areas where we can work together. Thus far, we are encouraged by the level of participation from both industries.

Since its formation, the partnership has moved quickly to establish objectives and a process through which to achieve them. As such, the partnership has established five working groups, each made up of experts from participating associations' member companies. Each working group will have a focus area on which members will work to advance a consensus opinion that improves overall security.

The working group areas of focus are:

1. Threat Information Sharing
2. Cybersecurity Risk Mitigation
3. Advanced Card-Present Security Technology
4. Card-Not-Present and Mobile Security
5. Cybersecurity and Data Breach Notification

Given the complexity of the issues under consideration, participating associations have worked to select the appropriate subject matter experts to represent the interests of their membership. Nominations have been received, groups have been populated with members, and the first meetings of the working groups will begin next week.

The tasks before these working groups are significant, but we believe they are achievable and we are committed to achieving significant progress by the end of 2014.

In closing, we believe that in working together with public and private sector stakeholders, our ability to develop innovative solutions and anticipate threats will grow, enhancing our collective security and giving our customers the service and peace of mind they deserve. I appreciate the opportunity to testify before you today and I look forward to your questions.

Testimony of
Tiffany O. Jones
iSIGHT Partners, Inc.

Before the
Senate Homeland Security and Governmental Affairs Committee

Regarding
"Data Breach on the Rise: Protecting Personal Information from Harm"

April 2, 2014

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, thank you for the opportunity to present to you today.

My name is Tiffany Jones, and I represent iSIGHT Partners, a leading cyber threat intelligence firm. Over the last seven years, we have built a team of 200+ experts dedicated to studying cyber threats in many nations across the globe and enabling organizations to protect themselves against these threats.

There are a variety of threat domains that make up the cyber threat landscape today. Each of these threat domains is motivated differently. For example, Cyber Espionage, targeted intrusion operations aimed at corporate and government entities to collect information for the purpose of a strategic advantage, can be politically motivated (stealing secrets) or economically motivated (stealing intellectual property). Cyber Hacktivism focuses on the intentions and capabilities of politically- or ideologically-motivated actors, who express their beliefs or attempt to project power through malicious or destructive online activity. Cyber Crime focuses on cyber threats from primarily financially-motivated actors.

The intelligence we research, analyze and disseminate, coupled with the scope, scale, and duration of the recent retailer attacks, leads us to one very clear conclusion: We need to stop thinking about cyber crime like the movie *Catch Me If You Can*, one clever young man assuming identities and passing bad checks.

Instead, we need to understand that cyber crime is more like the movie *Goodfellas*, an organized community of bad people, intent on crime, economically motivated, increasingly sophisticated, and operating without much fear of law enforcement.

Cyber crime is a global industry with a division of labor, evolved supply and demand, as well as a defined value chain. This chart gives you an overview of what that value chain looks like:

Step 1 – Malware: Cyber crime starts with malware. Think of this like an App Store for hackers. Thousands of developers craft hacking tools and toolkits with various features,

functions, and capabilities and sell them on a broad array of electronic markets. Prices can range from a few to several thousand dollars.

Just like an App Store, only a fraction of malware goes on to be popular depending upon the features, targeted vulnerability, usability, and other characteristics. At any point in time, there are probably a few thousand notable pieces of malware on the market with 10 new entrants that warrant analysis in a given month.

At higher price points – subscriptions of $5,000 to $15,000 per month – there is also private access to malware developers. These are the more sophisticated designers.

Step 2 – Infrastructure: Cyber criminals must obfuscate their operations. This means buying storage, computing, and network services from dedicated infrastructure operators – sort of a Criminal Cloud Computing. This is a large and varied segment of the market, everything from securing $50 domain names to $1,000 per server per month hosting arrangements. Some of these organizations can scale to multi-million dollar operations serving 1000+ criminal clients.

Step 3 – Cyber Crime Operators: Like entrepreneurs, operators assemble temporary teams, acquire tools, secure infrastructure, and execute against a plan. The better the plan, the bigger the payout. Like entrepreneurs, the very best exploit a market need, quickly monetize the value, and move on to the next opportunity. One recent operation netted as much as $3.8 million for the operator and their team in just a few short months.

Step 4 – Brokerages/Intermediaries: To monetize stolen assets in cyber crime – typically this is some form of personal data like credit card, health insurance, or social security numbers – the operators take their bulk data to brokers. Think of these players – again numbering in the thousands – as wholesalers.

The brokerages pay bulk prices to the operators for the stolen data, and then parcel it up into sizes that a larger number of smaller criminals can use. At the retail level, this looks like an underworld eBay, with prices set by the type, newness, quality, and completeness of the stolen data. More reliable sellers get higher prices.

In early December, we saw complete U.S. credit cards at $100 per card. With the dramatic increase in supply due to several recent retailer breaches, the price dropped to $50. Much of that card data is now dated and U.S. cards sell at closer to $16 per card.

Step 5 – Card Buyers & Mules: The transition from the criminal economy to the traditional economy presents the biggest bottleneck for cyber crime. Using stolen information involves risks and transaction costs, so most cyber criminals leave much of the small change on the table while focusing their efforts on big, quick hits. Card buyers and mules bear most of the risk.

The typical card buyer or a mule for receiving stolen property or bank payments is just a small-time, and occasionally unwitting, criminal – the intern of the cyber crime industry. They

get relatively small payments, if any, for relatively small crimes. They are typically involved in the illegal activity for a short time, and often have no connection with the larger criminal enterprise. Like a pickpocket who just takes the cash from your wallet – their gain is small, but your loss in time, effort, and personal value can be significant.

So, as you can see, the scope of the cyber criminal market is daunting – and the money made pales in comparison to economic value destroyed as a result. At any time, there are tens if not hundreds of thousands of independent actors. They are global. They are unregulated. They are better equipped, better trained, and more experienced than many of their law enforcement counterparts. And they are growing bolder.

You will see attacks like the 2013 retailer breaches again, and with greater frequency. Business and government has started to understand the scope of this problem, and are increasingly shifting to intelligence-led cyber security to improve prevention, speed response, and solve the cyber security risk equation. There is progress. There needs to be more of it. Thanks to government entities like Department of Homeland Security, USSS, and their awareness efforts, the severity and scope of the problem is becoming increasingly evident.

As you consider policy, here are some things to consider:

Don't:

- Seek to be technically prescriptive. Tools and tactics evolve too rapidly, so the policy responses need to be flexible. While EMV, or chip and pin, increases security on credit cards, it is not the panacea to solve all data breach problems. Additional measures, like encryption of data at rest as well as data in transit will also go a long way to protecting what the bad guys are really after: sensitive data.
- View this just as a technology problem. Cyber security, like traditional crime prevention and disaster preparedness, needs to be treated within the context of business and government management as a risk management issue.
- Equate the quantity of arrests in cyber crime with the quality of arrests – focused prosecution higher in the value chain makes a bigger impact

Do:

- Increase global collaboration. Most of these people are not inside of our borders. Without foreign law enforcement and community engagement, there will be no progress
- Focus the efforts on cyber risk management – the recent NIST framework is a good push in the right direction. Building threat more holistically into the risk framework is needed. If you do not understand your threat profile and the threats coming after you, you cannot solve for risk within your organization.
- Direct continuing NIST efforts to specifically evolve risk models that define a true ROI aligned to business/mission requirements

Thanks again for the opportunity to speak with you today. I look forward to answering any questions you may have.

The Cyber Crime Economy
An Underground Ecosystem

iSIGHTPARTNERS

Malware Developers

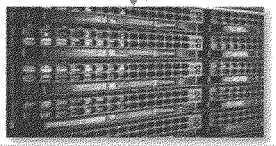
Cyber Crime Operators & Infrastructure Providers

Card Brokers

Card Buyers & Mules

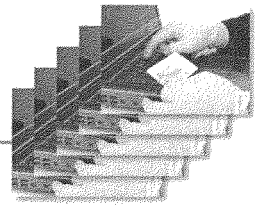
The App Store:
The price of a single piece of malware can range from a few to several thousand dollars.

The Entrepreneur:
There is the potential to make millions.

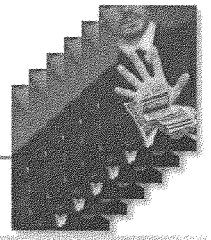


Criminal Cloud Computing:
Can scale to multi-million dollar operations serving 1000+ criminal clients.

The Online Auction of the Underworld:
More reliable sellers get higher prices.



The Interns:
Relatively small payments, if any, for relatively small crimes.



April 1, 2014

The Honorable Thomas Carper
Chairman
Committee on Homeland Security
United States Senate
513 Hart Senate Building
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security
United States Senate
172 Russell Senate Building
Washington, D.C. 20510

Dear Chairman Carper and Ranking Member Coburn:

We write today on behalf of the nation's food retailers and wholesalers to thank the Committee for its interest in data security in holding tomorrow's hearing entitled, "Data Breach on the Rise: Protecting Personal Information From Harm."

Customer safety is FMI's and our member companies' top priority. From the food we sell, to the personal payment data we handle, the food retail industry has invested significant financial, technical and human resources to ensure our customers' safety. The fact is that in spite of our and other industries' ongoing investment and commitment, the threat of criminal data breaches continues to grow. That threat expands beyond the payments chain, and into other areas of commerce, our universities, and government agencies that are threatened daily by cyber-attacks.

FMI is working with our members to share information about potential threats, lessons learned, and success stories in dealing with cyber-crime. We are developing best practices guidelines as a resource for our members as they continue to find new innovative ways to protect customer data, and if in the case of a breach, to mitigate the damage as much as possible. Furthermore, earlier this year we released a position paper on the grocery industry's commitment to customer safety, and principles that will help protect data moving forward. I have attached FMI's paper to this letter, and respectfully request that it is submitted for the record of this hearing.

Finally, FMI is actively engaged in the newly formed Merchant – Financial Services Cybersecurity Partnership. FMI sees this as an opportunity for all links in the payments chain to work together in exchanging information and finding real solutions to protect consumer data on an ongoing basis.

Thank you again for your work in the area of data security. We look forward to working with this committee on this very important issue.

Sincerely,

Jennifer Hatcher
Senior Vice President
Government and Public Affairs

cc: U.S. Senate, Members, Committee on Homeland Security

2345 Crystal Drive, Suite 800, Arlington, VA 22202-4801 T 202.452.8444 F 202.429.4519 www.fmi.org

FMI
THE VOICE OF FOOD RETAIL
Feeding Families Enriching Lives

Grocers' Commitment to Customers' Payment Data Security

Consumer Safety
Customer safety is the supermarket industry's top priority.

From the safety of the food we sell, to the safety and security of our customers and their payment and shopping data, the grocery industry is committed to protecting our customers.

There is no failsafe technology to protect against breaches for any type of company. Even companies that spend millions on data security and meet and exceed current standards and protocols for data protection can still find themselves victims of a criminal breach. Unfortunately, this is a fact of the modern marketplace. Supermarket retailers and wholesalers are committed to taking every step possible to prevent breaches, and if they do occur, identify them quickly and mitigate any damage to customers as soon as possible.

Coordinating With Law Enforcement
It is essential that private industry be able to tap into the expertise of law enforcement to try to identify potential breaches and then work to track down and prosecute the criminals who are behind them.

Opportunities to Improve Electronic Payments
The supermarket industry stands ready to work with all stakeholders in the payments chain – processors, credit card companies, equipment manufacturers and banks – to find real improvements that increase customer data security. Today's solutions and future technological improvements will need buy-in by all parties to ensure customer data is protected throughout the payments system.

PIN & Chip
One technology that has been successful in Europe and Canada is the implementation of EMV, or personal identification number (PIN) and chip-enabled credit and debit cards. This technology reduces the risks associated with breaches by making it more difficult to counterfeit cards and/or add unauthorized users. Grocers support the universal implementation in the U.S. payment card system of PIN security along with chip-embedded cards. We do not support chip and signature-only because it is a missed opportunity to add an important layer of protection to ensure the correct user is authorized to use the card.

Utilizing Emerging Technology
The current magnetic stripe card utilizes 1960's technology while PIN and chip uses more advanced, but also proven, technology developed roughly twenty years ago. While both systems may still have a place in payments for the near future, advancements in technology are quickly making magnetic stripe cards obsolete. Grocers are excited about the future of payments, and the opportunities mobile payments offer to bring greater security to the payments system. Mobile devices offer opportunities to leverage dynamic, tokenized payment data. This technology would reduce or eliminate the use of actual account numbers or credentials. Instead, it employs one-time tokens and sophisticated algorithms to ensure that sensitive data within the system is of no use to criminals seeking to compromise consumer accounts in the event of a breach.

Mobile also offers additional user verification solutions, such as biometrics or two-factor authentication and user location technology, all of which add additional layers of security.

January 2014

2345 Crystal Drive, Suite 800, Arlington, VA 22202-4801 T 202.452.8444 F 202.429.4519 www.fmi.org

April 2, 2014

Data Breach on the Rise: Protecting Personal Information from Harm

On behalf of the nearly 7,000 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing titled: "Data Breach on the Rise: Protecting Personal Information from Harm." Community bankers and their customers are deeply alarmed by the recent, wide-scale data breaches at prominent, national retail chains. These breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system. This confidence is vital to sustaining consumer spending necessary for the economic recovery. It is critical we determine what happened, identify the weakest links in the payments processing chain, and implement targeted changes to enhance consumer financial data security. We appreciate the opportunity to offer the community bank perspective on this important issue.

Making Customers Whole

In the wake of the retailer breaches, community banks have reissued more than four million credit and debit cards to consumers at a total reissuance cost of more than $40 million.[1] Reissuance costs are higher for community banks than for larger institutions that take advantage of economies of scale. Community banks absorb these costs upfront, even though the breaches occurred with retailers, because their primary concern is to protect their customers. Ultimately, these costs should be borne by the party at fault for the breach. This change would strengthen incentives for data protection. Because community banks acted quickly, initial fraud costs were relatively low. Less than one percent of community bank customers reported fraud on their accounts as a result of the recent breaches. These consumers are protected by a policy of zero-liability coverage. Financial institutions are required to provide this protection in order to issue Visa and MasterCard debit and credit cards.

While our current focus is on making customers whole, it is appropriate to begin to consider changes in policy, business practices, and technology that will strengthen payment system security and curb the risk of future breaches. The Joint Cybersecurity Partnership, joining ICBA and other financial services and retailer trade organizations, holds the promise of strengthening much needed cooperation across the payments chain.

More Comprehensive Data Security Standards Are Needed

Since 1999, financial institutions have been subject to rigorous data protection standards under the Gramm-Leach-Bliley Act (GLBA). These standards have been effective in securing consumer data at financial institutions. To adequately protect consumers and the payments system, **all** participants in the payments system should be subject to GLBA-like standards. Under current law, merchants and other parties that process or store consumer financial data are not subject to federal data security standards. Securing financial data at banks is of limited value if it remains exposed at the point-of-sale and other processing points.

[1] Numbers are based on a sampling of community banks.

1615 L Street NW, Suite 900, Washington, DC 20036 ▪ 202-659-8111 ▪ Fax 202-659-9216 ▪ www.icba.org

Liability Should Be Used To Align Incentives

To maximize data security, the party that experiences a breach should bear responsibility for all costs associated with the breach. This change would better align incentives to keep consumer data safe and foster good business practices. As described above, when payment card information is compromised, mitigation costs are significant. If the party that experiences the breach does not bear these costs, they have little incentive to improve their data security.

National Data Security Breach and Notification Standard is Vital

Most states have enacted laws with differing requirements for protecting customer information and giving notice in the event of a data breach. This patchwork of state laws only increases burdens and costs, fosters confusion, and ultimately is detrimental to customers. Customer notification is important so that individuals can take steps to protect themselves from identity theft or fraud. However, notification requirements should allow financial institutions and others flexibility to determine when notice is useful and appropriate. An overly broad notification standard that requires notice even when no threat exists will blunt the impact of notices that signal actual risk. Federal banking agencies should set the standard for financial institutions, as they currently do.

To that end, ICBA is encouraged by the introduction of S. 1927, the Data Security Act of 2014, by Chairman Carper and Senator Blunt. S. 1927 recognizes the value of the rigorous data security protocols of the GLBA that already apply to community banks and other financial institutions while also calling for uniform national standards to replace the current patchwork of federal and state data security standards. We look forward to working with Chairman Carper, Senator Blunt and others on this important legislation.

New Technologies Will Reduce Risk But There Is No Universal Remedy

Community banks are already investing in technologies that will better secure transaction processing and thwart criminals. In particular, community banks are joining other financial institutions in the orderly migration to chip technology for debit and credit cards. Chip technology may not have prevented the recent retailer breaches but it would have reduced the market value of the card data as it would be far more difficult for criminals to make counterfeit cards. Using chip technology will not protect against fraud in "card-not-present" transactions, such as online purchases. Criminals will continue to try to find weakness regardless of the technology so it is crucial that the marketplace continues to have the flexibility to innovate.

Thank you again for convening this hearing. ICBA looks forward to working with this Committee to craft targeted solutions to enhance the safety and security of consumer financial data.

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org
National Association of Federal Credit Unions | www.nafcu.org

April 1, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security &
Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security &
Governmental Affairs
United States Senate
Washington, D.C. 20510

Re: ***Protecting Personal Consumer Information from Data Breaches***

Dear Chairman Carper and Ranking Member Coburn:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federal credit unions, I write in advance of tomorrow's hearing, "*Data Breach on the Rise: Protecting Personal Information from Harm.*" We appreciate the committee's focus on this issue in the wake of a concerning string of data breaches at merchants.

As the number of data breaches at U.S. retailers continues to climb, so does the emotional toll and financial burden on tens of millions of consumers across the country. The colossal scale of recent data breaches continues to demonstrate the necessity for Congressional action. Since the Target breach became public, we have seen a steady stream of other large data breaches making national headlines.

As you know, in recent testimony before Congress witnesses from both Target and Neiman Marcus admitted that they were not able to detect their own system breaches; Target was alerted by the Department of Justice and Neiman Marcus by their card processor. NAFCU believes this alarming fact should be further examined as entities must be capable of protecting their own systems in order to protect consumers.

The recent Target breach of over 110 million records has been especially onerous on credit unions. Our member credit unions report that, on average, they have received hundreds of inquiries from their members seeking assistance due to the recent Target breach. NAFCU estimates that this particular breach could end up costing the credit union community nearly $30 million. This cost comes from fraud monitoring, reissuance of cards and actual losses from this breach. It does not even count the intangible cost of the staff time needed to handle all of the member service issues that stem from the breach. Unfortunately, credit unions will likely never recoup much of this cost, as there is no statutory requirement on merchants to be accountable for costs associated with breaches that result on their end.

These numbers echo what has historically happened to credit unions when a major retailer data breach occurs. A recent survey of NAFCU-member credit unions found that the 2006 data breach at TJ Maxx stores led to a median cost of $32,000 per institution from the breach, with only about 10% of those costs ever recovered on average.

As we first wrote to Congress in February 2013, as part of NAFCU's five-point plan on regulatory relief, there is a need to data security to be addressed by lawmakers. Every time consumers choose to use plastic cards for payments at a register or make online payments from their accounts, they unwittingly put themselves at risk. Many are not aware that their financial and personal identities could be stolen or that fraudulent charges could appear on their accounts, in turn damaging their credit scores and reputations. Consumers trust that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, this is not always true.

Financial institutions, including credit unions, have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act*. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, and they become victims of data breaches and data theft all too often. While these entities still get paid, financial institutions bear a significant burden as the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum standards for protecting such data.

NAFCU supports legislation introduced by Chairman Carper and Senator Blunt, the *Data Security Act of 2014* (S. 1927), that would make great strides toward ensuring that a strong federal standard is in place to protect sensitive financial data. The bill is an excellent first step toward addressing ongoing data breaches at retailers across the country. NAFCU appreciates the bill's sponsors for recognizing that credit unions are already subject to strict data security protections under the *Gramm-Leach Bliley Act* and including language to ensure they are not subject to any new onerous or duplicative regulation under the proposed law.

The need for legislation to bring additional entities, including merchants that handle sensitive consumer information into the federal regulatory rubric was underscored recently by estimates that one-third of the American public has been adversely impacted by the breaches disclosed over the last few months. While these breaches have drawn national attention, the reality is that data breaches are happening all the time, often on a smaller scale that does not make the nightly news. When taken together, these smaller breaches impact just as many consumers. According to the Identity Theft Resource Center, there were more than 600 reported data breaches in 2013 – a 30 percent increase over 2012. The business sector accounted for almost 82 percent of the breached records while the financial sector accounted for less than 2 percent of all breached records in 2013.

A recent Javelin Strategy & Research report (December 2013) found that financial institutions are doing a much better job than retailers when it comes to credit card security. "Retailers, common targets for data breach crimes, scored the lowest in prevention and among the lowest overall," said Al Pascual, the senior analyst who co-authored the report. Furthermore, according to the Verizon 2013 Data Breach Investigation Report, a breakdown of incidents across various industries actually resulting

from network intrusions, the retail industry was far and away the number one target, with nearly 22 percent of network intrusions occurring at retailers.

While some argue for financial institutions to expedite the switch to "chip and PIN" technology, the reality is that it is no panacea for data security and preventing merchant data breaches. Many "chip and PIN" cards were compromised in the Target data breach because the terminals at the point of sale only accepted magnetic stripe technology. "Chip and PIN" technology does not protect against online fraud, as the technology is designed to hinder in-person fraud and card duplication. Besides, from what some in the retail industry have recently suggested, a financial institution switching to the new technology will likely not mean that retailers make the move with them. Tom Litchford, vice president of retail technologies at the National Retail Federation, recently told *The Wall Street Journal* (March 26, 2014, "Retail Association: Card Security Costs Outweigh Benefits for Many") that CIOs must weigh whether the costs to upgrade their payment systems are greater than the financial costs associated with fraud and that many retailers would upgrade on their own pace, based on the return on investment.

As long as retailers are more concerned with their bottom line than protecting consumers, no one should expect their personal data to be protected. This is yet another fact highlighting the need for greater national data security standards as the way to truly help protect consumer financial information.

NAFCU continues to recommend that Congress make the following priorities in any legislation and act on the following issues related to data security:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *Gramm-Leach-Bliley Act*.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes 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.

- **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.

- **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 disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones 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 merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **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 merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

On behalf of our nation's credit unions and their 97 million members we thank you for your attention to this important matter. Again, we urge you to hold retailers to the same strict standards of data security and breach notification that financial institutions must adhere to. We look forward to working with your offices on existing legislation and new ideas as the legislative process takes shape. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Associate Director of Legislative Affairs, Chad Adams, at (703) 842-2265.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Committee on Homeland Security & Governmental Affairs

STATEMENT OF THE

NATIONAL RETAIL FEDERATION

FOR THE

SENATE COMMITTEE ON

HOMELAND SECURITY & GOVERNMENT AFFAIRS

HEARING ON

"DATA BREACH ON THE RISE:

PROTECTING PERSONAL INFORMATION FROM HARM"

APRIL 2, 2014

National Retail Federation
101 New York Avenue, N.W., Suite 1200
Washington, D.C. 20005
(202) 783 –7971
www.nrf.com

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

Chairman Carper, Ranking Member Coburn, members of the Committee, on behalf of the National Retail Federation (NRF) we want to thank you for giving us this opportunity to provide you with these comments on data security and protecting American's financial information. NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy.

Collectively, retailers spend billions of dollars safeguarding consumers' data and fighting fraud. Data security is something that our members strive to improve every day. Virtually all of the data breaches we've seen in the United States during the past couple of months – from those at retailers that have been prominent in the news to those at banks and card network companies that have received less attention – have been perpetrated by criminals that are breaking the law. All of these companies are victims of these crimes and we should keep that in mind as we explore this topic and public policy initiatives relating to it.

This issue is one that we urge the Committee to examine in a holistic fashion: we need to reduce fraud. That is, we should not be satisfied with deciding what to do after a data breach occurs – who to notify and how to assign liability. Instead, it's important to look at why such breaches occur and what the perpetrators get out of them so that we can find ways to reduce and prevent not only the breaches themselves, but the fraudulent activity that is often the goal of these events. If breaches become less profitable to criminals then they will dedicate fewer resources to committing them and our goals will become more achievable.

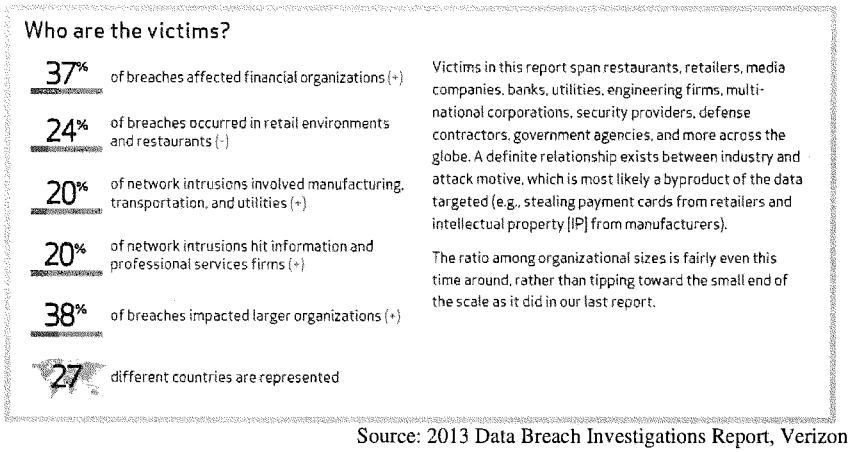
With that in mind, these comments are designed to provide some background on data breaches and on fraud, explain how these events interact with our payments system, discuss some of the technological advancements that could improve the current situation, raise some ways to achieve those improvements, and then discuss the aftermath of data breaches and some ways to approach things when problems do occur.

Data Breaches in the United States

Unfortunately, data breaches are a fact of life in the United States. In its 2013 data breach investigations report, Verizon analyzed more than 47,000 security incidents and 621 confirmed data breaches that took place during the prior year. Virtually every part of the economy was hit in some way: 37% of breaches happened at financial institutions; 24% happened at retail; 20% happened at manufacturing, transportation and utility companies; and 20% happened at information and professional services firms.

It may be surprising to some given recent media coverage that more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area. There are hundreds of times as many merchants accepting card payments in the United States than there are financial institutions issuing and processing those payments. So, proportionally, and not

surprisingly, the thieves focus far more often on banks which have our most sensitive financial information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.



Source: 2013 Data Breach Investigations Report, Verizon

Nearly one-fifth of all of these breaches were perpetrated by state-affiliated actors connected to China. Three in four breaches were driven by financial motives. Two-thirds of the breaches took months or more to discover and 69% of all breaches were discovered by someone outside the affected organization.[1]

These figures are sobering. There are far too many breaches. And, breaches are often difficult to detect and carried out in many cases by criminals with real resources behind them. Financially focused crime seems to most often come from organized groups in Eastern Europe rather than state-affiliated actors in China, but the resources are there in both cases. The pressure on our financial system due to the overriding goal of many criminals intent on financial fraud is acute. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality.

Background on Fraud

Fraud numbers raise similar concerns. Just a year ago, Forbes found that Mexico and the United States were at the top of the charts worldwide in credit and debit card fraud.[2] And fraud losses in the United States have been going up in recent years while some other countries have had success reducing their fraud rates. The United States in 2012 accounted for nearly 30 percent of

[1] 2013 Data Breach Investigations Report, Verizon.
[2] "Countries with the most card fraud: U.S. and Mexico," *Forbes* by Halah Touryalai, Oct. 22, 2012.

credit and debit card charges but 47 percent of all fraud losses.[3] Credit and debit card fraud losses totaled $11.27 billion in 2012.[4] And retailers spend $6.47 billion trying to prevent card fraud each year.[5]

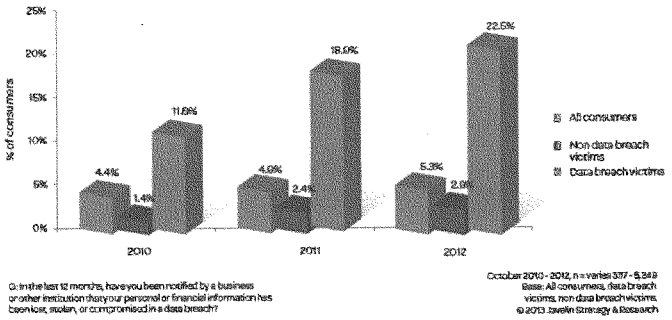
Fraud is particularly devastating for retailers in the United States. LexisNexis and Javelin Strategy & Research have published an annual report on the "True Cost of Fraud" each year for the last several years. The 2009 report found, for example, that retailers suffer fraud losses that are 10 times higher than financial institutions and 20 times the cost incurred by consumers. This study covered more than just card fraud and looked at fraudulent refunds/returns, bounced checks, and stolen merchandise as well. Of the total, however, more than half of what merchants lost came from unauthorized transactions and card chargebacks.[6] The founder and President of Javelin Strategy, James Van Dyke, said at the time, "We weren't completely surprised that merchants are paying more than half of the share of the cost of unauthorized transactions as compared to financial institutions. But we were very surprised that it was 90-10."[7] Similarly, Consumer Reports wrote in June 2011, "The Mercator report estimates U.S. card issuers' total losses from credit- and debit-card fraud at $2.4 billion. That figure does not include losses that are borne by merchants, which probably run into tens of billions of dollars a year."[8]

Online fraud is a significant problem. It has jumped 36 percent from 2012 to 2013.[9] In fact, estimates are that online and other fraud in which there is no physical card present accounts for 90 percent of all card fraud in the United States.[10] And, not surprisingly, fraud correlates closely with data breaches among consumers. More than 22 percent of breach victims suffered fraud while less than 3 percent of consumers who didn't have their data breached experienced fraud.[11]

---

[3] "U.S. credit cards, chipless and magnetized, lure global fraudsters," by Howard Schneider, Hayley Tsukayama and Amrita Jayakumar, *Washington Post*, January 21, 2014.
[4] "Credit Card and Debit Card Fraud Statistics," CardHub 2013, available at http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/.
[5] *Id.*
[6] A fraud chargeback is when the card-issuing bank and card network take the money for a transaction away from the retailer so that the retailer pays for the fraud.
[7] "Retailers are bearing the brunt: New report suggests what they can do to fight back," by M.V. Greene, NRF Stores, Jan. 2010.
[8] "House of Cards: Why your accounts are vulnerable to thieves," Consumer Reports, June 2011.
[9] 2013 True Cost of Fraud, LexisNexis at 6.
[10] "What you should know about the Target case," by Penny Crosman, *American Banker*, Jan. 23, 2014.
[11] 2013 True Cost of Fraud, LexisNexis at 20.

Figure 11. Fraud Incidence Rate Among All Consumers, Data Breach Victims, And Non Data Breach Victims (2010 -2012)



Source: 2013 True Cost of Fraud, LexisNexis

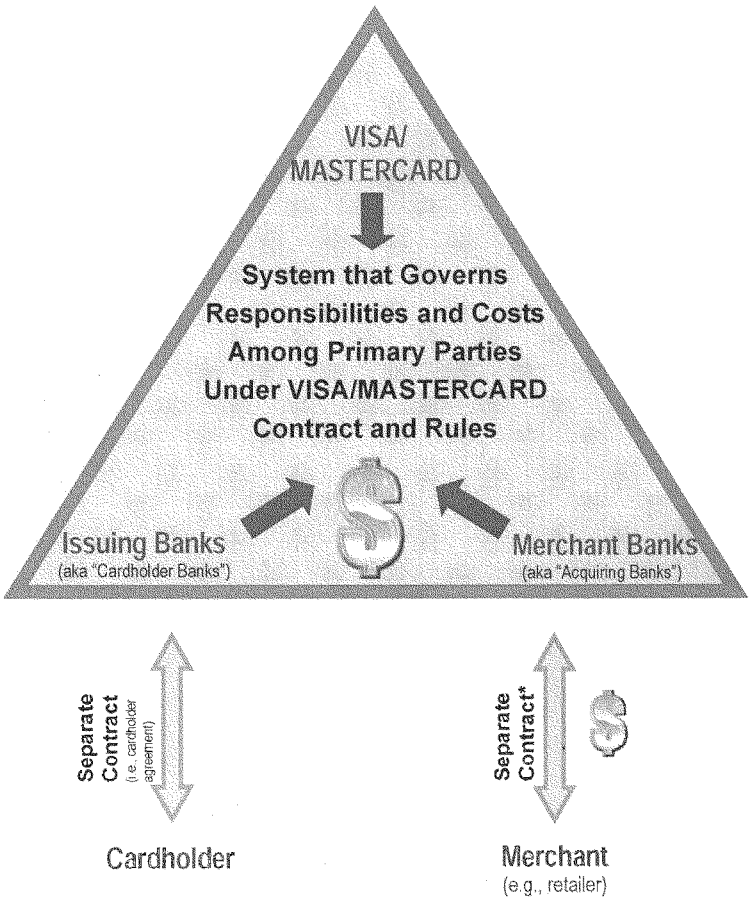
These numbers provide insights as to how to get to the right solutions of better safeguarding consumer and cardholder data and the need to improve authentication of transactions to protect against fraud. But before delving into those areas, some background on our payments system could be helpful.

The Payments System

Payments data is sought in breaches more often than any other type of data.[12] Now, every party in the payment system, financial institutions, networks, processors, retailers and consumers, has a role to play in reducing fraud. However, although all parties have a responsibility, some of those parties are integral to the system's design and promulgation while others, such as retailers and consumers, must work with the system as it is delivered to them.

As the following chart shows, while the banks are intimately connected to Visa and MasterCard, merchants and consumers have virtually no role in designing the payment system. Rather, they are bound to it by separate agreements issued by financial intermediaries.

[12] 2013 Data Breach Investigations Report, Verizon at 445, figure 35.



* Typically contract between merchant bank and its retailers requires retailers to reimburse merchant bank for any costs, penalties, or fees imposed by the system on the merchant bank (including chargebacks – i.e., disputed charges – and costs of data breaches)

Thus consumers are obligated to keep their cards safe and secure in their wallets and avoid misuse, but must necessarily turn their card data over to others in order to effectuate a transaction.

Retailers are likewise obligated to collect and protect the card data they receive, but are obligated to deliver it to processors in order to complete a transaction, resolve a dispute or process a refund. In contrast, those inside the triangle have much more systemic control.

For example, retailers are essentially at the mercy of the dominant credit card companies when it comes to protecting payment card data. The credit card networks – Visa, MasterCard, American Express, Discover and JCB – are responsible for an organization known as the PCI (which stands for Payment Card Industry) data security council. PCI establishes data security standards (PCI-DSS) for payment cards. While well intentioned in concept, these standards have not worked quite as well in practice. They have been inconsistently applied, and their avowed purpose has been significantly altered.

PCI has in critical respects over time pushed card security costs onto merchants even when other decisions might have more effectively reduced fraud – or done so at lower cost. For example, retailers have long been required by PCI to encrypt the payment card information that they have. While that is appropriate, PCI has not required financial institutions to be able to accept that data in encrypted form. That means the data often has to be de-encrypted at some point in the process in order for transactions to be processed.

Similarly, merchants are expected to annually demonstrate PCI compliance to the card networks, often at considerable expense, in order to benefit from a promise that the merchants would be relieved of certain fraud inherent in the payment system, which PCI is supposed to prevent. However, certification by the networks as PCI Compliant apparently has not been able to adequately contain the growing fraud and retailers report that the "promise" increasingly has been abrogated or ignored. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote recently, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history."[13]

PCI has not addressed many obvious deficiencies in cards themselves. There has been much attention to the fact that the United States is one of the last places on earth to put card information onto magnetic stripes on the backs of cards that can easily be read and can easily be counterfeited (in part because that data is static and unchanging). We need to move past magstripe technology.

But, before we even get to that question, we need to recognize that sensitive card data is right on the front of the card, embossed with prominent characters. Simply seeing the front of a card is enough for some fraudsters and there have been fraud schemes devised to trick consumers into merely showing someone their cards. While having the embossed card number on the front of the card might have made sense in the days of knuckle-buster machines and carbon copies, those days are long passed.

In fact, cards include the cardholder's name, card number, expiration date, signature and card verification value (CVV) code. Everything a fraudster needs is right there on the card. The

[13] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/.

bottom line is that cards are poorly designed and fraud-prone products that the system has allowed to continue to proliferate.

PCI has also failed to require that the identity of the cardholder is actually verified or authenticated at the time of the transaction. Signatures don't do this. Not only is it easy to fake a signature, but merchants are not allowed by the major card networks to reject a transaction based on a deficient signature. So, the card networks clearly know a signature is a useless gesture which proves nothing more than that someone was there purporting to be the cardholder.

The use of personal identification numbers (PINs) has actually proven to be an effective way to authenticate the identity of the cardholder. PIN numbers are personal to each cardholder and do not appear on the cards themselves. While they are certainly not perfect, their use is effective at reducing fraud. On debit transactions, for example, PIN transactions have one-sixth the amount of fraud losses that signature transactions have.[14] But PINs are not required on credit card transactions. Why? From a fraud prevention perspective, there is no good answer except that the card networks which set the issuance standards have failed to protect people in a very basic way.

As noted by LexisNexis, merchant fraud costs are much higher than banks' fraud costs. When credit or debit card fraud occurs, Visa and MasterCard have pages of rules providing ways that banks may be able to charge back the transaction to the retailer (which is commonly referred to as a "chargeback"). That is, the bank will not pay the retailer the money for the fraudulent transaction even though the retailer provided the consumer with the goods in question. When this happens, and it happens a lot, the merchant loses the goods *and* the money on the sale. According to the Federal Reserve, this occurs more than 40 percent of the time when there is fraud on a signature debit transaction,[15] and our members tell us that the percentage is even higher on credit transactions. In fact, for online transactions, which as noted account for 90 percent of fraud, merchants pay for the vast majority of fraudulent transactions.[16]

Retailers have spent billions of dollars on card security measures and upgrades to comply with PCI card security requirements, but it hasn't made them immune to data breaches and fraud. The card networks have made those decisions for merchants and the increases in fraud demonstrate that their decisions have not been as effective as they should have been.

Improved Technology Solutions

There are technologies available that could reduce fraud. An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-and-

---

[14] *See* 77 Fed. Reg. 46261 (Aug. 3, 2012) reporting $1.11 billion in signature debit fraud losses and $181 million in PIN debit fraud losses.
[15] *Id.* at 46262.
[16] Merchants assume 74 percent of fraud losses for online and other card-not-present signature debit transactions. 77 Fed. Reg. 46262.

mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Canada, for example, is exploring the use of a PIN for online purchases. The same should be true here. Doing so would help directly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

Protecting all cards with a PIN instead of a signature is the single most important fraud protection step that could be taken quickly. It's proven, it's effective, and it's relatively easily implementable. PIN debit cards are close to ubiquitous worldwide, and readily producible in the U.S. Chip is desirable add-on. If speed of implementation is of importance, then substituting PIN for signature is preferable to implementing Chip. More than twice as many U.S. terminals are ready to accept PIN cards today, than are chip ready. Despite this, one major card brand continues to denigrate PINs in favor of signature, in part because they can collect more fees with fraud-prone signature transactions.[17]

Cards should also be smarter and use dynamic data rather than magnetic stripes. In much of the world this is done using computer chips that are integrated into physical credit and debit cards. It is important to note, however, that there are many types of technologies that may be employed to make this upgrade. EMV, which is an acronym for Europay, MasterCard and Visa, is merely one particular proprietary technology. As the name indicates, EMV was established by Europay, MasterCard and Visa. A proprietary standard could be a detriment to the other potentially competitive networks.[18] Adopting a closed system, such as EMV, means we are locking out the synergistic benefits of competition.

But even within that closed framework, it should also be noted that everywhere in the world that EMV has been deployed to date the card networks have required that the cards be used with a PIN. That makes sense. But here, the dominant card networks are proposing to force chips (or even EMV) on the U.S. market without requiring PIN authentication. Doing that makes no sense and loses a significant part of the fraud prevention benefits of chip technology. To do otherwise would mean that merchants would spend billions to install new card readers without they or their customers obtaining PINs' fraud-reducing benefits. We would essentially be

---

[17] See Appendix A. This document was unsealed in 2010 from the record of the *In re Visa Check/MasterMoney* antitrust litigation.

[18] There are issues with EMV because the technology is just one privately owned solution. For example, EMV includes specifications for near field communications that would form the technological basis of Visa and MasterCard's mobile payments solutions. That raises serious antitrust concerns for retailers because we are just starting to get some competitors exploring mobile payments. If the currently dominant card networks are able to lock-in their proprietary technology in a way that locks-out competition in mobile payments, that would be a bad result for merchants and consumers who might be on the verge of enjoying the benefits of some new innovations and competition.

So, while chip cards would be a step forward in terms of improving card products, if EMV is forced as the chip card technology that must be used – rather than an open-source chip technology which would facilitate competition and not predetermine mobile payment market-share – it could be a classic case of one step forward and two steps backward.

spending billions to combine a 1990's technology (chips) with a 1960's relic (signature) in the face of 21st century threats.

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, as noted earlier, not everyone in the payments chain is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require "end-to-end" (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form.

According to the September 2009 issue of the Nilson Report "most recent cyberattacks have involved intercepting data in transit from the point of sale to the merchant or acquirer's host, or from that host to the payments network." The reason this often occurs is that "data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can't accept encrypted data at this time."[19]

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place – at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. Likewise, using PIN-authentication of cardholders now would offer some additional protection against fraud should this decrypted payment data be intercepted by a criminal during its transmission "in the clear."

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the "token"). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.[20] Still, tokenization is not a panacea, and it is important that whichever form is adopted be an open standard so that a small number of networks not obtain a competitive advantage, by design, over other payment platforms

In many models tokenization occurs "after the fact" – generally post authorization. Thus some fraud risk remains. To deal with this point-to- point encryption is preferred and would be complimentary to tokenization. The former would occur between the card being read and the assignment of a token. From the merchant's perspective, tokenization involves significant operational changes and could carry significant out-of-pocket costs. Despite that, for the majority of transactions, tokenization still may not address both ends of the security/authentication equation as well as would PIN and Chip. It has greatest utility in the 6 percent of transactions that currently do not occur face-to-face. Consequently, while point-to-point encryption and tokenization could be valuable adjuncts to PIN and Chip authentication, they are not a substitute.

---

[19] The Nilson Report, Issue 934, Sept. 2009 at 7.

[20] For information on Shift4's 2005 launch of tokenization in the payment card space see http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit.

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers won't need to have a physical card – and they certainly won't replicate the security problem of physical cards by embossing their account numbers on the outside of their mobile phones. It should be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords. Indeed, if we are looking to leapfrog the already aging current technologies, mobile-driven payments may be the answer.

Indeed, as much improved as they are, chips are essentially dumb computers. Their dynamism makes them significantly more advanced than magstripes, but their sophistication pales in comparison with the common smartphone. Smartphones contain computing powers that could easily enable comparatively state-of-the-art fraud protection technologies. The phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

The dominant card networks have not made all of the technological improvements suggested above to make the cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe.

In this section, we have merely described some of the solutions available, but the United States isn't using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

A Better System

How can we make progress toward the types of solutions that would reduce the crimes of data theft and fraud? One thing seems clear at this point: we won't get there by doing more of the same. We need PIN-authentication of card holders, regardless of the chip technology used on newly issued cards. We also need chip cards that use open standards and allow for competition among payment networks as we move into a world of growing mobile commerce. Finally, we need companies throughout the payment system to work together on achieving end-to-end encryption so that there are no weak links in the system where sensitive card payment information may be acquired more easily than in other parts of the system.

Steps Taken by Retailers After Discovery of a Breach of Security

In our view, it is after a fulsome evaluation of data breaches, fraud, the payments system and how to improve each of those areas in order to deter and prevent problems that we should turn to the issue of what to do when breaches occur. Casting blame and trying to assign liability is, at

best, putting the cart before the horse and, at worst, an excuse for some actors to ignore their own responsibility for trying to prevent these crimes.

One cannot reasonably demand greater security of a system than the system is reasonably capable of providing. Some participants act as if the system is more robust than it is. Currently, when the existing card products are hit in a criminal breach, that company is threatened from many sides. The threats come from entities seeking to exact fines and taking other penalizing action even before the victimized company can secure its network from further breaches and determine through a forensic analysis what has happened in order to notify potentially affected customers. For example, retailers that have suffered a breach are threatened with fines for the breach based on allegations of non-compliance with PCI rules (even when the company has been certified as PCI-compliant). Other actors may expect the breached party to pay for all of the fraudulent transactions that take place on card accounts that were misused, even though the design of the cards facilitated their subsequent counterfeiting. Indeed, some have seriously suggested that retailers reimburse financial institutions for the cost of reissuing more fraud-prone cards. And, as a consequence of the breach, some retailers must then pay higher fees on its card transactions going forward. Retailers pay for these breaches over and over again, despite often times being victims of sophisticated criminal methods not reasonably anticipated prior to the attack.

Breaches require retailers to devote significant resources to remedy the breach, help inform customers and take preventative steps to ward off future attacks and any other potential vulnerabilities discovered in the course of the breach investigation. Weeks or months of forensic analysis may be necessary to definitively discover the cause and scope of the breach. Any discovered weaknesses must be shored up. Quiet and cooperative law enforcement efforts may be necessary in an effort to identify and capture the criminals. Indeed, law enforcement may temporarily discourage publication of the breach so as to not alert the perpetrators that their efforts have been detected.

It is worth noting that in some of these cases involving payment card data, retailers discover that they actually were not the source of the breach and that someone else in the payments chain was victimized or the network intrusion and theft occurred during the transmission of the payment card data between various participants in the system. For this reason, early attempts to assign blame and shift costs are often misguided and policy makers should take heed of the fact that often the earliest reports are the least accurate. Additionally, policy makers should consider that there is no independent organization devoted to determining where a breach occurred, and who is to blame – these questions are often raised in litigation that can last for years. This is another reason why it is best to at least wait until the forensic analysis has been completed to determine what happened. Even then, there may be questions unanswered if the attack and technology used was sophisticated enough to cover the criminals' digital tracks.

The reality is that when a criminal breach occurs, particularly in the payments system, all of the businesses that participate in that system and their shared customers are victimized. Rather than resort to blame and shame, parties should work together to ensure that the breach is remedied and steps are taken to prevent future breaches of the same type and kind.

Legislative Solutions

In addition to the marketplace and technological solutions suggested above, NRF also supports a range of legislative solutions that we believe would help improve the security of our networked systems, ensure better law enforcement tools to address criminal intrusions, and standardize and streamline the notification process so that consumers may be treated equally across the nation when it comes to notification of data security breaches.

From many consumers' perspective payment cards are payment cards. As has been often noted, consumers would be surprised to learn that their legal rights, when using a debit card – i.e. their own money – are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers' reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

In addition, NRF supports the passage by Congress of the bipartisan "Cyber Intelligence Sharing and Protection Act" (H.R. 624) so that the commercial sector can lawfully share information about cyber-threats in real-time and enable companies to defend their own networks as quickly as possible from cyber-attacks as soon as they are detected elsewhere by other business.

We also support legislation that provides more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

Finally, and for nearly a decade, NRF has supported passage of legislation that would establish one, uniform federal breach notification law that would be modeled on, and preempt, the varying breach notification laws currently in operation in 46 states, the District of Columbia and federal territories. A federal law could ensure that all entities handling the same type of sensitive consumer information, such as payment card data, are subject to the same statutory rules and penalties with respect to notifying consumers of a breach affecting that information, Further, a preemptive federal breach notification law would allow retailers and other businesses that have been victimized by a criminal breach to focus their resources on remedying the breach and notifying consumers rather than hiring outside legal assistance to help guide them through the myriad and sometimes conflicting set of 50 data breach notification standards in the state and federal jurisdictions. Additionally, the use of one set of standardized notice rules would permit the offering to consumers of the same notice and the same rights regardless of where they live.

Conclusion

In closing three points are uppermost.

First, retailers take the increasing incidence of payment card fraud very seriously. We do so as Main Street members of the community, because it affects our neigbbors and our customers. We do so as businesses, because it affects the bottom line. Merchants already bear at least an

equal, and often a greater, cost of fraud than any other participant in the payment card system. We have every reason to want to see fraud reduced, but we have only a portion of the ability to make that happen. We did not design the system; we do not configure the cards; we do not issue the cards. We will work to effectively upgrade the system, but we cannot do it alone.

Second, the vast majority of breaches are criminal activity. The hacked party, whether a financial institution, a card network, a processor, a merchant, a governmental institution, or a consumer is the victim of a crime. Traditionally, we don't blame the victim of violence for the resulting stains; we should be similarly cautious about penalizing the hackee for the hack. The payment system is complicated. Every party has a role to play; we need to play it together. No system is invulnerable to the most sophisticated and dedicated of thieves. Consequently, eliminating all fraud is likely to remain an aspiration. Nevertheless, we will do our part to help achieve that goal.

Third, it is long past time for the U.S. to adopt PIN and chip card technology. The PIN authenticates and protects the consumer and the merchant. The chip authenticates the card to the bank. If the goal is to reduce fraud we must, at a minimum, do both.

Appendix A

EXHIBIT 499

Visa U.S.A. Inc.

Debit Advisors Meeting

Phoenix, Arizona
February 28 - March 1, 1990

Agenda

Wednesday, February 28	
Continental Breakfast	7:30 a.m. - 8:00 a.m.
Welcome and Introduction	8:00 a.m. - 8:15 a.m.
UK Market Update	8:15 a.m. - 8:45 a.m.
Review of Merchant Visits/ FMI and Research Update	8:45 a.m. - 9:15 a.m.
Fraud Experts Conclusions	9:15 a.m. - 9:45 a.m.
Break	9:45 a.m. - 10:00 a.m.
Product Concept "Z," Version 3	10:00 a.m. - 10:45 a.m.
Group Session Introduction	10:45 a.m. - 11:00 a.m.
Group Sessions	11:00 a.m. - 12:00 noon
Lunch	12:00 noon - 1:00 p.m.
Group Sessions (continued)	1:00 p.m. - 4:30 p.m.
Cocktail Reception and Dinner	6:00 p.m.
Thursday, March 1	
Continental Breakfast	8:00 a.m. - 8:30 a.m.
Group Presentations and Discussion	8:30 a.m. - 10:00 a.m.
Break	10:00 a.m. - 10:15 a.m.
Business Case Review	10:15 a.m. - 11:30 a.m.
Wrap-up	11:30 a.m. - 12:00 noon

307

Visa U.S.A. Inc.

Debit Advisors Meeting

Phoenix, Arizona
February 28 - March 1, 1990

Table of Contents

UK MARKET UPDATE

The banks in the United Kingdom have recently introduced debit products into their marketplace, which is a well established credit card market. The combination of the product positioning and marketing caused significant merchant backlash resulting in major price concessions by the banks.

To provide background for the Advisors' discussions on debit product introduction into the U.S. market, a presentation will be given covering these events in the UK.

REVIEW OF MERCHANT VISITS

The "Z" debit product concept was defined by Visa and presented to the Advisory Committee in November 1989. To better assess the marketability of the service, it was determined that the "Z" product concept should be shared with the merchant community. Because November and December were such busy months for retailers, a wide-scale merchant survey was impractical during this time. However, it was decided that a limited number of on-site merchant interviews could be accomplished quickly.

Therefore, during the month of December 1989, Visa and Global Concepts visited ten (10) merchants to better understand their payment operations, and to solicit their opinions on a variety of debit card attributes such as PINs, signatures, electronic returns, tiered offerings including a guarantee, service value, target marketing, etc.

The ten (10) merchants that were visited are shown below:

Company	Location	Contact
Safeway	San Francisco, CA	Melanie Hobden
Ralph's	Los Angeles, CA	Roger Borneman
Farm Fresh	Norfolk, VA	Glenn Sharpe
Giant Food	Landover, MD	Mike Mann
Exxon	Houston, TX	Richard Phegley
Texaco (telephone)	Houston, TX	Ken Zell
Southland	Dallas, TX	Keith Jenkins
Circle K	Phoenix, AZ	Anita Best
Radio Shack	Fort Worth, TX	Virginia Meyer
Target	Minneapolis, MN	Carrie Lichtenberg

In most cases the acquiring Visa bank provided the contact name at the merchant, and in some instances the acquirer even participated in the interview.

The purpose of the visits was to test the "Z" product attributes against both the current merchant payment procedures and their desired future payment procedures.

A presentation to review the major findings will be made at the meeting.

FRAUD EXPERTS CONCLUSIONS

PROJECT OBJECTIVES AND SCOPE

The primary objectives of the fraud project and the January 9-11, 1990, fraud experts meeting are to identify and rank fraud risks associated with the "Z" debit product concept that is currently under development by Visa U.S.A. Merchant, acquirer and issuer fraud risks are included in this evaluation. Additionally, the experts will specify controls for the fraud risks they identify and rank.

SELECTION CRITERIA FOR EXPERTS

"Z" does not currently exist in the marketplace; therefore, experts from related fields are evaluating fraud risks associated with the product concept.

Professionals from Visa Member banks, retailers from food and oil companies, industry vendors and Visa Security & Risk Management staff experts are participating in the project. They are recognized experts on POS debit, credit card, ATM and check fraud and are principally senior business managers with direct responsibility for risk management and/or fraud at their companies.

METHODOLOGY

A modified Delphi technique, a set of procedures designed to balance individual expert opinions with group consensus, was used to develop a consensus among industry fraud experts. The process is as follows:

Round 1: Development of Individual Positions

Prior to the group meeting, each expert was asked to develop their own fraud position based on their interpretation of the debit product concept. A questionnaire was sent to each expert on December 15, 1989, to rank fraud risks associated with the proposed debit product. The completed questionnaires were returned to Visa, consolidated and summarized for the Fraud Experts Meeting in January.

Round II: Development of Group Positions

Through group and breakout discussions at the January meeting, group positions were developed. Individuals contributed to one another's understanding of the issues and the difficulties involved, and personal opinions were refined as a result of Round II discussions. Individual and group opinions were discussed to eliminate misinterpretations and to bring to light knowledge available from one or a few members of the group. To facilitate this process, the format was:

- At the onset of the meeting, experts with divergent views presented their positions and the group discussed them.

- The experts were then grouped together with several of their peers to discuss their individual positions and develop a joint opinion.
- Each of the three small groups reported on their position to the entire group, differences were questioned and a consensus position developed.

Additionally, each expert completed a second questionnaire following the small group discussions.

Rounds III and IV: Finalization of Experts' Consensus

Two post meeting questionnaires were completed by the fraud experts on January 19 and February 15, 1990. The group consensus included in the project report is the position that resulted from the final, Round IV questionnaire.

INTERIM PRESENTATION TO DEBIT ADVISORS

An interim presentation will be given to the Debit Advisors at the end of February 1990 in which the experts' ranking of fraud risks to merchants, acquirers and issuers will be reviewed. Additionally, the January meeting and final fraud report will be reviewed.

FINAL REPORT

The final report will be published at the end of March 1990. It will include the experts' ranking of fraud risks, their consensus on key fraud issues, a comparison of the Debit Advisors' fraud survey and experts' consensus, a summary of the January meeting, the results of the four Delphi questionnaires, the results of the Debit Advisors Fraud Survey, biographies for the fraud experts and related background information and data.

PRODUCT CONCEPT "Z," VERSION 3

Mark

Separate from Visa bands design

Signifies POS only, not an ATM mark

Signifies debit only

Coexistence with Visa logo not permitted

Third party ACH product option not acceptable

Market

Universally issued

Medium value positioning to consumers

National issuance and acceptance

Displaces cash and checks

Point of Sale Operations

Tiered service levels

- Issuer Guaranteed (Primary service)
- Non-Guaranteed (Secondary service)
  Merchant downtime and override
  - Stand-alone service not necessary for product launch

Tiered merchant risk commensurate with price

Tiered issuer risk commensurate with interchange fee income

PIN and signature for cardholder identification

Critical Mass

Compatible with BASE I/II and Debit System

Compatible with current ATM network systems

GROUP SESSION INTRODUCTION

Brief presentations will be made to the group to explain the benefits of an on-line debit product ("Z") and an off-line debit product (Visa Debit). Following this the advisors will break into two working groups and will be asked to identify all positive aspects of only one of the products as well as the drawbacks. If possible, the group should work to resolve the drawbacks. The group may also wish to discuss reasons why the other product, which is being supported by the other working group, will not work in the marketplace.

A list of the working groups and the product each will be asked to support follows:

Off-line Debit Product Group	**On-line Debit Product Group**
Debby McWhinney, Leader	Tommy Lewis, Leader
Joel Crabtree	Loraine Boland
John Davis	Bob Copeland
Denny Dumler	Bill Fackler
Dave Fronek	Phil Heasley
Fran Gormley	Steve Iovino
Bil Lyons	Jimmy Lewin
Ken Rosfeld	Lynn Page
John Thompson	John Sikkink
Staff	
Wes Tallman	Gerald Hawke
Jeanne Schapp	Mary Buckley
Allen Lipis	Steve White
Chris Schellhorn	Joel Friedman

GROUP SESSIONS

PRESENTATION NOTES

Off-line Debit Product

- Internationally recognized logo
- Existing operational infrastructure
- Proven profitability
  - Merchant discount income
  - Interchange fee income
  - Cardholder fees
- Fourteen years of experience in the marketplace
  - Issuance
  - Acceptance
- Signifies acceptance at POS locations worldwide
  - Existing merchant base, 7 million
- Signifies acceptance at ATMs worldwide
  - Existing ATM network, 40,000

On-line Debit Product

- Universally issued
- Appeals to non-plastic accepting merchants
  - Cash and check
  - High transaction volume
  - Repeat business
- Safest product for banks, less fraud
- Safest product for consumers
- Carries the best guarantee for merchants
- Provides ability for merchants to fully integrate payment mechanism with their other automation activities
- Eliminates need to store paper
- Compatible with existing ATM network procedures
- Will benefit from future economies of scale
  - Costs will come down
  - Income will increase
- Consumer friendly
  - Ease to use
  - Eliminates bulky checkbook

GROUP PRESENTATIONS AND DISCUSSION

Enhanced presentations on the off-line and on-line debit products will be given. Following discussion, individuals will be asked to accept or reject either alternative and provide reasons for their selection.

BUSINESS CASE REVIEW

Visa has hired Andersen Consulting to assist in the development of a business case for debit at the point of sale. A presentation will be made explaining the process, the major business assumptions that have been made, and the current status.

Post-Hearing Questions for the Record
Submitted to The Honorable Edith Ramirez
From Senator Tom Coburn

"Data Breach on the Rise: Protecting Personal Information from Harm"
April 2, 2014

1. Are you concerned that private companies will be unwilling to report data breaches to the federal government for fear of being prosecuted?

   Information sharing is an important part of the fight against those who attempt to exploit consumers' personal information, and one key consideration is how best to encourage industry participation. For example, a number of industries have established Information Sharing and Analysis Centers (ISAC) to enable industry members to pool information about security threats, defenses so that they can prepare for new kinds of attacks, and quickly address potential vulnerabilities. To be most effective, ISACs may receive information from, and share information with, relevant government agencies. The FTC has been exploring, at the request of members of Congress, the formation of an ISAC for the retail industry, and the Retail Industry Leaders Association recently announced the launch of such a program to allow retailers to share threat information with other retailers, government agencies including law enforcement agencies, and financial institutions.

   We also would expect companies to comply with requirements, whether under existing state laws in the majority of states or under a federal statute, to report data breaches despite the potential for legal action by banks, individual consumers, or government agencies, such as the FTC or state attorneys general.

2. Is it reasonable to hold private companies to an arguably higher standard than government agencies, especially given the recent IG and GAO reports detailing the lapses in government agency's cyber security?

   Federal agencies are generally subject to data security standards similar to those required for the private sector. Under the Federal Information Security Management Act (FISMA), agencies must have policies that consider "the risk and magnitude of the harm" that would result from unauthorized access or use. OMB and DHS oversee agencies' implementation of these standards. NIST also develops technical data security standards and guidelines for government information systems.

   OMB guidance also requires agencies to have plans to determine whether to notify individuals if there is a breach of their personal information. One of the primary criteria is whether there is a "reasonable risk of harm." In addition, under federal law (FISMA) and OMB guidance, agencies must report cybersecurity incidents to US-CERT at DHS in accordance with DHS guidance.

3. In your written testimony you state that a strong national breach notification law is preferable to state notification laws. Why do you believe this is so and of what do you think a strong national requirement should consist?

The FTC supports federal legislation that would (1) strengthen its existing data security tools and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.

While a majority of states have data breach notification laws, few have specific laws requiring general data security policies and procedures. Breach notification and data security standards at the federal level would extend notifications to all citizens nationwide and ensure a strong and consistent national standard that would simplify compliance by businesses while protecting all American consumers.

4. Do you agree there should be a delay in any breach notification by a company to afford the company the opportunity to identify the nature of the breach, to discern what information has been compromised, and to provide law enforcement an opportunity to investigate, if necessary?

Prior to giving notice, companies that suffer a data breach should have an opportunity to determine the scope of the breach and identify those consumers whose information may have been compromised. In light of the harms that consumers may suffer from such an incident, however, this should be done without unreasonable delay so that companies can provide consumers notice as soon as practicable so that they can take action to protect themselves.

5. Under a national breach notification law, how long do you believe a company should have before they are required to notify customers of a breach?

Notice should be provided as soon as practicable and without unreasonable delay. We also support the inclusion of an outer limit for notification, such as 30 or 60 days.

6. How do the FTC and USSS work together when confronting major data breaches, such as those that recently occurred at Target, Neiman Marcus and Michaels?

The FTC works with federal criminal agencies, including USSS, when investigating data breaches. For example, in some instances, criminal law enforcement agencies have asked us to delay our investigation so as not to impede a criminal investigation, and we have honored such requests.

The goals of the FTC and criminal agencies are complementary. FTC actions send a message that businesses need to protect their customers' data on the front end, and actions by criminal agencies send a message to identity thieves that their efforts to victimize consumers will be punished. This approach to data security leverages government resources and best serves the interests of consumers.

For example, in its case against retailer TJX, the Commission alleged that the company's failure to use basic security measures resulted in a hacker obtaining tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. Banks also

claimed that tens of millions of dollars in fraudulent charges were made, and cancelled and reissued millions of cards. At the same time, the Justice Department successfully prosecuted a hacker behind the TJX breach.

7. Most of the recent legislation on data breach addresses what private entities should be required to do when confronted with a security breach. However, the federal government holds an enormous amount of Americans' personal information. Before we proscribe standards by which the private sector must abide, in what areas do you believe Congress should require additional data security standards for federal agencies?

As discussed above, federal agencies are subject to data security standards similar to those required for the private sector. OMB and DHS oversee implementation of FISMA, which requires agencies to have policies that consider "the risk and magnitude of the harm" that would result from unauthorized access or use. To meet these standards, agencies must tailor their policies based on a number of factors, such as the type and sensitivity of the data in question. OMB guidance also requires agencies to have plans to determine whether to notify individuals if there is a breach of their personal information. And, under FISMA and OMB guidance, agencies must report cybersecurity incidents to the US Computer Emergency Readiness Team (US-CERT) at DHS in accordance with DHS guidance.

   a. Could you provide an example from your agency in which additional standards would be helpful in protecting the personal information your agency maintains?

Existing federal standards provide the FTC with sufficient ability to protect personal information that it maintains. The FTC has policies and procedures in place for safeguarding the confidentiality, privacy, and security of FTC records, information, and data, whether maintained in electronic format on FTC IT systems or media or in paper format. These policies and procedures are tailored to the type and sensitivity of the data in question.

Post-Hearing Questions for the Record
Submitted to William Noonan
From Senator Tom A. Coburn, M.D.

"Data Breach on the Rise: Protecting Personal Information from Harm

April 2, 2014

Question#:	1
Topic:	bad guys
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Are we doing enough to stop the "bad guys" or adversaries who commit cybercrimes? What additional powers or resources do you believe are required by the Secret Service in order to more aggressively investigate and deter through arrest cybercrime?

Response: The Secret Service has 30 years of experience investigating cybercrime, and over this time period we have discovered, responded to, and investigated the most costly known cybercrimes in history—these are: the data breaches of TJX in 2007, Heartland Payment Systems in 2009, and the recent Target data breach. In total, over the past four years the Secret Service has arrested approximately 4,900 cyber criminals and prevented an estimated $12 billion in potential fraud losses through these investigations. However, despite present efforts to counter cybercrime, the Secret Service assesses that transnational organized cybercrime has continued to grow in scale and sophistication over the past ten years, and that this growth will likely continue despite the disruptive impact of present efforts.

Investigating cybercrime primarily requires skilled criminal investigators. The Secret Service's cyber programs are scalable with a proven record of training and developing Secret Service special agents into highly capable cybercrime investigators. However, over the past three years, the Secret Service workforce has been reduced by over 650 personnel, nearly ten percent of our total workforce. Recruiting, training, deploying, and retaining the special agents needed to advance Secret Service's cyber programs is a key priority in our FY 2014 to FY 2018 Strategic Plan.

The cyber investigative efforts of the Secret Service would be further assisted by legislative changes like those proposed by the Administration's May 2011 legislative proposal, which proposed revisions to keep Federal criminal law up-to-date. We continue to support changes like these that will keep up with rapidly-evolving technologies and uses.

Question#:	2
Topic:	cybercrime investigations
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: How many agents do you have devoted to cybercrime investigations? What manpower level do you feel would be necessary in order to investigate all cybercrimes under your jurisdiction?

Response: Through an integrated mission and organization, the Secret Service efficiently accomplishes its protective responsibilities,[1] its law enforcement responsibilities related to the U.S. financial system,[2] and the investigation of cybercrime.[3] Since 2008, the Secret Service has trained all of its agents in the investigation of cybercrimes through its Basic Investigation of Computers and Electronic Crimes course as part of their initial training. The Secret Service also provides advanced training to special agents for investigating cybercrimes through its Electronic Crimes Special Agent Program (ECSAP). At present, the Secret Service has approximately 280 special agents active in this program and has developed plans to increase this number to 600 over multiple years of increased training. In FY 2013, the Secret Service recorded man hours directed towards cybercrime investigations totaling approximately 260 FTEs. Additionally, since 2008, the Secret Service has annually increased its cybercrime investigative efforts—as measured by special agent man hours.

The total occurrence of violations of the principle cybercrime laws assigned to Secret Service jurisdiction, 18 USC §§ 1029-1030, far exceeds the current capacity of the Secret Service. The 2014 Verizon Data Breach Investigations Report identified more than 63,000 confirmed cybersecurity incidents including 1,367 confirmed data breaches in 2013. Many of these potentially violate cybercrime laws under the Secret Service's jurisdiction. However, instead of reactively investigating each incident, the Secret Service proactively targets and investigates the most capable cyber criminals who are responsible for the most significant and costly data breaches.

[1] See 18 USC § 3056 (a) & (e)
[2] See 18 USC § 3056(b)
[3] See 18 USC §§ 1029-1030

Question#:	3
Topic:	resources
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: How many cases or incidents do you decide not to investigate due to a lack of resources? Or, in the alternative, how many more cases could you investigate if you had more resources?

Response: Given the total volume of cybersecurity incidents, rather than reactively investigating these incidents, the Secret Service proactively investigates the most capable cyber criminals. Incrementally scaling the capacity of the Secret Service may provide proportional benefit in our efforts to investigate cyber criminals. In 2013, as a result of the efforts of approximately 260 FTEs who were involved in cybercrime investigations, the Secret Service arrested over 1,080 cyber criminals who, in total, were responsible for $235 million in fraud losses. The Secret Service conservatively estimates these arrests prevented over $1.1 billion in fraud losses based on the payment card data exposed. In FY 2013, the Secret Service used approximately $76 million in budget resources as part of its cybersecurity efforts; the majority of this was personnel costs. We will continue to evaluate our allocation of resources across our mission spaces and target the most capable cyber criminals.

Question#:	4
Topic:	USSS's investigations
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Based on the USSS's investigations, what do you estimate is the probability of being caught and convicted of cybercrime?

Response: The Secret Service is dedicated and patient in investigating cybercrime. Through Secret Service's cyber investigations, we have discovered previously unknown large scale data breaches, which have generated criminal profits totaling tens and hundreds of millions of dollars in illicit revenue, and have identified and apprehended many of the most capable cyber criminals. Those who are involved in high-consequence cybercrimes are eventually identified and apprehended by the Secret Service; however, these investigations require a long-term focus and may take years to accomplish.

Over the past four years Secret Service cybercrime cases that have gone to prosecution have averaged over a 99.5% conviction rate. However, it is impossible to establish an over all probability of the risk of a cyber criminal being apprehended, as it varies greatly depending on the efforts of the criminal to avoid law enforcement. The Secret Service continues to see growth in transnational cybercrime, as a result of the challenges inherent in international law enforcement investigations including the need for cooperation from foreign law enforcement to obtain evidence and apprehend offenders. The Secret Service continues enhance foreign law enforcement cooperation and develop the cyber investigative capabilities of foreign law enforcement, while developing innovative investigative programs to bring transnational cyber criminals to justice in the United States.

Question: How do you think the probability of being caught influences hackers or other criminals' decisions to commit these types of crime?

Response: The risk of being caught certainly influences cyber criminals' decisions. The Secret Service has observed criminals move into cybercrime due to a perceived lower risk of apprehension and opportunities for substantial illicit profits. Due to the risk of being caught, experienced cyber criminals expend tremendous effort to avoid detection and select targets they believe are less likely to result in their apprehension. As a result of transnational reach of cyberspace combined with effective law enforcement domestically, the Secret Service has seen an on-going growth in transnational organized cybercrime in countries with little cyber investigative capacity or a history of limited international law enforcement cooperation.

Question#:	4
Topic:	USSS's investigations
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Due to the impact of apprehension, law enforcement is a critical component of our Nation's cybersecurity strategy. In addition to deterring the individual cybercriminal, effective law enforcement disrupts the cybercrime underground, defeating the networks and organizations that are required for conducting the most high consequence cybercrimes and developing the capability of novice cyber criminals. For this reason, the Secret Service applies a strategic targeted approach to identify key individuals and nodes supporting organized cybercrime and arrest them and seize critical evidence to identify and disrupt their cybercrime schemes. For example, in May 2013 the Secret Service shut down Liberty Reserve, which is alleged to have had more than one million users worldwide and to have laundered more than $6 billion in criminal proceeds.

Question: Should the federal government be doing more to try to deter cyber criminals from conducting these attacks? If so, how?

Response: Current research on the cost of cybercrime indicates that preventing cybercrime through investigations, arrest, and deterrence is an effective means to reduce the aggregate economic cost of cybercrime.[4] The Secret Service assesses that most of the major cyber criminals are outside of the United States and operate as part of transnational cybercrime networks. Investigating these transnational networks, and cooperating with foreign law enforcement to apprehend and disrupt their operations, is a key priority of the Secret Service's cyber investigations program, which has resulted in numerous highly notable arrests of transnational cyber criminals. A critical component of this is continuing to foster international law enforcement partnerships and cooperation in investigating cybercrime through the efforts of Secret Service's international field offices and the Department of State.

[4] See for example Anderson, et al. "Measuring the Cost of Cybercrime." Workshop on the Economics of Information Security WEIS 2012 (June 2012). Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Question#:	5
Topic:	FTC and USSS
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: How do the FTC and USSS work together when confronting major data breaches, such as those that recently occurred at Target, Neiman Marcus and Michaels?

Response: The Secret Service coordinates with various government agencies with responsibilities related to the crimes that the Secret Service investigates, including the Federal Trade Commission (FTC). However, the purposes of Secret Service investigations are substantially different from the FTC—we are focused on identifying and apprehending the cyber criminals responsible and not on determining if the victim organization was in compliance with the data security provisions under the FTC's regulatory jurisdiction. Additionally, the Secret Service widely shares general information concerning cybercrime trends, tactics, and best security practices while protecting victim privacy and civil rights and civil liberties.

Question#:	6
Topic:	data breach cases 1
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: There is clearly a balance between the need to provide public disclosure of a breach and the need to keep information confidential for a period of time to avoid tipping off the cyber criminals of your investigation. How important is it to your investigations of data breach cases that you have sufficient time to conduct your analysis prior to public notification of the breach?

Response: It is often critically important that law enforcement is able to delay public disclosure of data breaches for a period of a few days or weeks, in order to develop investigative leads while also working to prevent or minimize fraud losses, or other direct financial losses, from occurring. The Secret Service has detected and investigated cybercrimes where the eagerness of a victim to publically disclose a data breach risked preventing the Secret Service from recovering the data and minimizing the risks of its fraudulent use. It is for this reason the Secret Service supports a national data breach notification standard that would require reporting to an appropriate law enforcement agency and allows law enforcement to delay any public disclosure if this would impede a criminal investigation.

Question#:	7
Topic:	data breach cases 2
Hearing:	Data Breach on the Rise: Protecting Personal Information From Harm
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: How much time does the USSS spend investigating data breaches at federal agencies versus those at private businesses, if any? How do you prioritize your investigative resources between private and public data breach cases?

Response: The Secret Service prioritizes its cyber investigations to target the most capable cybercriminal organizations. These criminals are primarily motivated by greed and target organizations that possess sensitive financial information that is able to be monetized. The Secret Service has investigated and apprehended cyber criminals that have conducted data breaches on the networks of federal, state, local, and privately owned computer systems. The Secret Service does not prioritize its investigations based upon the victim of a particular data breach, but based on the capability demonstrated by the cyber criminals involved and the potential economic impact.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 20, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: GAO Response to Post-Hearing Questions on Cybersecurity

Dear Mr. Chairman:

It was a pleasure to appear before your Committee on April 2, 2014 to discuss federal agency responses to data breaches.[1] This letter responds to a request that I provide answers to post-hearing questions from Senator Coburn for the record. The questions, along with my responses, follow.

1. Should the American people be confident that federal agencies will protect their personal information?

a. For example, when people file their taxes this year, should they be confident the IRS will protect their personal information?

Under the Federal Information Security Management Act of 2002 (FISMA), agencies are required to establish information security programs that protect the security of information and systems in their custody on the basis of identified risks. However, as we reported in September 2013,[2] agencies have made mixed progress in implementing the components of these programs. In some areas agencies made advances in 2012, while in other areas there were setbacks. Overall, IGs at 21 of the 24 major federal agencies covered by the CFO Act cited information security as a major management challenge for their agency.

More specifically in regard to protecting personal information, agencies have reported increasing numbers of data breaches involving personally identifiable information (PII). As we noted in our testimony statement, the total number of reported PII data breaches at federal agencies has more than doubled recently, from 10,481 in 2009 to 25,566 in 2013. We have made a number of recommendations to specific agencies we reviewed to improve their responses to data breaches involving PII,[3] including recommending that agencies (1) consistently document risk levels and how those levels are determined for PII-related data

[1] GAO, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches*, GAO-14-487T (Washington, D.C.: Apr. 2, 2014).

[2] GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, GAO-13-776 (Washington, D.C.: Sep. 26, 2013).

[3] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

breaches; (2) document the number of affected individuals for each incident; and (3) identify lessons learned from responses to PII breaches. Agencies varied in the extent to which they concurred with the recommendations.

Regarding IRS protection of taxpayer information, we reported in April 2014[4] that while IRS had resolved a number of information security control weaknesses previously reported by GAO, significant risks remained. For example, the agency had not always (1) installed appropriate patches on all databases and servers to protect against known vulnerabilities, (2) sufficiently monitored database and mainframe controls, or (3) appropriately restricted access to its mainframe environment. In addition, IRS had allowed individuals to make changes to mainframe data processing without requiring them to follow established change control procedures to ensure changes were authorized; and did not configure all applications to use strong encryption for authentication, increasing the potential for unauthorized access. We concluded that until IRS takes additional steps to correct these and other problems, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure. We recommended that IRS update its policies and procedures for documenting access to information systems; develop a remedial action plan to address known weaknesses; and take 23 actions to correct weaknesses related to the use of cryptography and configuration management. IRS agreed to develop a detailed corrective action plan to address each recommendation.

2. On April 1st, Politico announced "more than 7 million people signed up for health insurance through Affordable Care Act exchanges through Monday night's deadline...and that number doesn't include sign-ups that took place in recent days through state exchanges." Should those who signed up for healthcare through HealthCare.gov be confident in the security of their health records and/or information they provide to HealthCare.Gov?

At Senator Coburn's request and the request of other members of Congress, we are currently conducting a review of the security and privacy of Healthcare.gov and the systems that support its operations. We are still in the early stages of that review and have not yet drawn any conclusions about how well personal information provided to Healthcare.gov is protected. We expect that our report, due out later this year, will address the question of whether the Centers for Medicaid and Medicare Services have implemented appropriate security and privacy controls for the site and the systems that directly support it.

3. Would you say the federal government is a model to follow for cyber security and data breach reporting?

Federal law and the information security-related standards and guidelines issued by the National Institute of Standards and Technology (NIST) provide a comprehensive framework for managing information security risks. Consistent with leading practices, this framework serves as a model for federal agencies in developing their information security programs. However, most agencies have not yet fully or consistently implemented their security programs, which continue to exhibit weaknesses. Our September 2013 report on compliance with FISMA showed mixed progress in implementing the requirements of the act. We and inspectors general continue to identify weaknesses in elements of agency programs. Most major federal agencies have had weaknesses in major categories of information security controls, as defined by our *Federal*

[4] GAO, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk*, GAO-14-405 (Washington, D.C.: Apr. 8, 2014).

Information System Controls Audit Manual, such as implementation of specific security controls.[5]

Regarding data breach reporting, agencies have demonstrated model behavior in only certain aspects of their programs, while other aspects need improvement. The Office of Management and Budget (OMB) and NIST have established requirements for responding to and reporting on data breaches that include key management and operational practices. These can be considered model practices for federal agencies to follow. In our review of eight agencies we determined that, with few exceptions, the agencies addressed the key management and operational practices in their policies and procedures. However, they did not consistently implement the operational practices. We have made recommendations to these agencies to improve the effectiveness of their data breach programs.

4. It has been reported that some federal agencies still operate Windows XP, which Microsoft has stopped providing updates and patches for this month. Does this present a security risk? Could this lead to data breaches?

All operating system software, including Windows XP, is susceptible to flaws in software code that could cause the program to malfunction or create security vulnerabilities. These flaws generally result from programming errors that occur during software development. As reported by NIST, based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. When vulnerabilities are discovered, software developers often develop code or patches to rectify the associated coding flaws and enhance the security and integrity of the software program. However, based on announcements made by Microsoft, it is likely that Microsoft will not continue to provide security updates and technical support for Windows XP in the future. Although Microsoft provided an update for a flaw in Internet Explorer on May 1, 2014, it stated that the update was made as an exception to its policy of no longer providing updates to Windows XP because of the proximity to the end date for such support. Microsoft noted that from a security standpoint today's threats have outpaced the ability to protect those customers using an operating system that dates back over a decade. If further security updates are not available, computers running Windows XP may become vulnerable to harmful viruses, spyware, and other malicious software, which can steal or damage stored data and information. Unless agencies that continue to use Windows XP take additional measures to extend software developer support or otherwise compensate for the lack of support, their information may be at a heightened risk of unauthorized disclosure, modification, and loss.

5. Do you think that the federal government is over-reporting some data breach incidents? If so, how can we strike a balance to ensure that significant cyber security or data breach incidents are reported to DHS, OMB, and/or the Congress, while not requiring agencies to report incidents that do not present a significant risk of data breach or exposure?

We believe the manner in which incidents are reported can be adjusted to conserve scarce agency resources without having adverse impact. As we reported in December 2013,[6] OMB's guidance to agencies requires them to report each data breach involving PII to the U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security

[5] GAO, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G (Washington, D.C.: Feb. 2009).

[6] GAO-14-34.

(DHS) within 1 hour of discovery. However, complete information from most incidents can take days or months to compile; therefore preparing a meaningful report within 1 hour can be infeasible. US-CERT officials stated they can generally do little with the information typically available within 1 hour and that receiving the information at a later time would be just as useful. Likewise, US-CERT officials said they have little use for case-by-case reports of certain kinds of data breaches, such as those involving paper-based PII, because they considered such incidents to pose very limited risk. As a result, agencies may be expending resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches. We recommended that the Director of OMB revise reporting requirements for PII-related breaches to US-CERT to include time frames that better reflect the needs of individual agencies and the government as a whole as well as consolidated reporting of incidents that pose limited risk. OMB neither agreed nor disagreed with our recommendation.

6. The DHS Office of Inspector General has produced audits examining the Department of Homeland Security's compliance with FISMA, identifying some areas where DHS remains non-compliant with FISMA. Some of the issues identified by the DHS OIG have been reported for multiple years. Given DHS's important delegated role in FISMA compliance for OMB and other federal agencies, what actions would you recommend DHS take to improve its own FISMA compliance to ensure that sensitive information is not exposed to data breach?

We have not conducted a comprehensive assessment of the information security program in place at DHS and thus do not have current recommendations to DHS to address department-wide issues regarding compliance with FISMA. In our September 2013 report we noted that metrics developed by DHS do not evaluate all FISMA requirements, such as conducting risk assessments and developing security plans; are focused mainly on compliance rather than effectiveness of controls; and in many cases did not identify specific performance targets for determining levels of implementation. We recommend that the Director of OMB, in coordination with the Secretary of Homeland Security, develop metrics for inspectors general to report on the effectiveness of agency information security programs. Since this is a DHS responsibility, DHS could enhance both its own program as well as other federal information security programs by improving these metrics.

In preparing this correspondence, we relied primarily on previously issued GAO products. We also reviewed recent public announcements by Microsoft Corporation regarding its Windows XP operating system. Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-6244, or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at wilshuseng@gao.gov and deferrarij@gao.gov, respectively.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

FINANCIAL SERVICES ROUNDTABLE

Post-Hearing Questions for the Record
Submitted to The Honorable Tim Pawlenty
From Senator Tom Coburn

"Data Breach on the Rise: Protecting Personal Information from Harm"
April 2, 2014

1. **Do you think that the federal government is investing enough in investigating and arresting cyber criminals?**

While the Financial Services Roundtable (FSR) and its technology division, BITS, appreciates the work of our nation's law enforcement officials, we believe the federal government has not invested enough in resources and personnel to enable the effective investigation, arrest, and successful prosecution of cyber criminals. Much more is needed.

In his March 12, 2013, testimony before the Senate Select Committee on Intelligence, Director of National Intelligence James Clapper warned:

> "So, when it comes to the distinct threat areas, our statement this year leads with cyber. And it's hard to overemphasize its significance.
>
> Increasingly, state and non-state actors are gaining and using cyber expertise. They apply cyber techniques and capabilities to achieve strategic objectives, by gathering sensitive information from public and private sector entities, controlling the content and flow of information, and challenging perceived adversaries of cyber space.
>
> These capabilities put all sectors of our country at risk—from government and private networks to critical infrastructures."[1]

Then FBI Director Robert Mueller and CIA Director John Brennan each testified similarly. While Director Mueller stated that the cyber threat keeps him "awake" at night[2], Director Brennan added that "the seriousness and the diversity of the threats that this country faces in the cyber domain are increasing on a daily basis.

[1] http://www.gpo.gov/fdsys/pkg/CHRG-113shrg82721/pdf/CHRG-113shrg82721.pdf at p.9.
[2] Ibid. at p.65.

FINANCIAL SERVICES ROUNDTABLE

And from my perspective, I think this is one of the real significant national security challenges we face. And the threat is going to continue, and it's going to grow"[3].

However, according to the Department of Justice's recent "Budget and Performance Submission," the number of full-time DOJ employees devoted to "combating cyber-based threats and attacks" for 2013 was only 35 full-time employees at a total cost of $7,643,000.[4] For 2014 (even after the resolution of the "sequester"), that number only rose by two to 37 full-time employees for a total cost of $8,080,000.[5] Such a low number of devoted personnel is clearly insufficient.

2. What recommendations would you make for federal agencies to do a better job deterring or stopping cyber crime?

As suggested above, Congress should provide federal agencies with resources commensurate with the threat. In terms of assisting the private sector in protecting and mitigating against the commission of cyber crimes, the FSR/BITS offers the following actionable recommendations for the federal government:

- Promote Information Sharing – While our sector – the financial services sector –continues to improve information sharing among sector members, significant progress requires congressional actions to enhance, facilitate, and protect threat information sharing across sectors and with government. Specifically, information sharing laws should be modernized to provide targeted protection from liability and public disclosure for entities that, in good faith, share threat information relating to defending consumers, the financial system, and our nation's critical infrastructure. We cannot overstate the importance to our industries and our customers of the need for this type of legislation. Removing the obstacles to information sharing will improve our ability to stop attacks in real time and prevent attacks from occurring in the first place. It is important to note that the purpose for such legislation is to protect consumers, individuals, and organizations by enabling the sharing of threat information, not to share sensitive or personal information. FSR supported the "Cyber Intelligence Sharing and

[3] Ibid. at p.54.
[4] http://www.justice.gov/jmd/2015justification/pdf/crm-justification.pdf at Exhibit D
[5] Ibid.

FINANCIAL SERVICES ROUNDTABLE

Protection Act of 2013"(commonly known as CISPA) that passed the House, and is supportive of the Senate Select Committee on Intelligence's efforts at crafting effective and workable information sharing legislation.

- Improve the Security Clearance Process – To further facilitate information sharing, FSR recommends that the federal government appropriately increase the number of security clearances for financial services executives and streamline the overall process so that these crucial frontline responders can promptly receive and act on critical, time-sensitive information.

- Update the US Criminal Code and Enhance Penalties – Statutes such as the Computer Fraud and Abuse Act (CFAA) were drafted and passed prior to much of our nation's dependence on network reliant critical infrastructure. In its current form, the CFAA does not set mandatory minimum penalties for criminal actions that could destroy or disrupt the confidentiality, integrity, or availability of backbone information systems of our critical infrastructure. The CFAA should be amended to establish minimum penalties that are commensurate with the harm caused.

- Engage the International Community – Physical proximity is no longer essential to commit a cyber crime. With a click of a mouse, a cyber criminal can damage crucial control systems or steal money and intellectual property from a hemisphere away. Accordingly, collaboration between U.S. and foreign governments in these matters is essential. Specifically, federal law enforcement provides legal and technical assistance to foreign counterparts and the U.S. Government can also work with other governments to enforce consequences for cyber crimes.

- Promote Existing Government-Private Sector Relationships That Work – As one of the oldest and most regulated sectors, the financial services sector has developed an effective working relationship with the U.S. Department of Treasury over the course of this nation's history. The federal government should maintain this relationship by continuing Treasury's designation as our "Sector Specific Agency" and primary agency for designating critical infrastructure components.

- Educate the Public – It is vital to improve public understanding of their role in fighting cybercrime and improve education of our nation's workforce and consumers regarding safe computing practices.

Other actionable recommendations include increased funding for cybersecurity research and development, development of workforce expertise in cybersecurity, and protection of personal and proprietary information through appropriate access restrictions for information within the custody and control of government agencies.

3. What role, if any, should the government play in encouraging the private sector to strengthen data security?

    a. If there is a role, how can the government both set an example for the private sector in the area of data security and provide businesses the flexibility they need within any federal guidance rather than burdensome regulations?

First and as noted above, passing legislation that encourages information sharing through targeted liability protections would immensely assist the private sector in strengthening its cybersecurity posture.

Second, while most FSR member companies are required to maintain the security and confidentiality of consumer information (see Title V, subtitle A of the Gramm-Leach-Bliley Act), the same cannot be said for millions of other entities that similarly and regularly handle sensitive consumer financial data. Other entities should also be held accountable for protecting sensitive financial account information.

Third, the federal government could encourage the private sector to strengthen cybersecurity by acting as a better example. However, as noted in the submitted testimonial statement of GAO Director Gregory Wilshusen:

- "only one of seven [federal] agencies reviewed [by the Government Accountability Office for its December 2013 report] had documented both an assigned risk level and how that level was determined for [personally identifiable information] data breaches; two agencies documented the

FINANCIAL SERVICES ROUNDTABLE

number of affected individuals for each incident; and two agencies notified affected individuals for all high-risk breaches.

- "the seven agencies did not consistently offer credit monitoring to affected individuals; and
- "none of the seven agencies consistently documented lessons learned from their breach responses."[6]

The federal government should follow the GAO recommendations that accompanied the December 2013 report[7] and act as an example in enhancing its own cybersecurity posture.

Lastly, the federal government could act as a convener for the private sector as the National Institute of Standards and Technology (NIST) did when it brought a myriad of private sector representatives together to help develop the Cybersecurity Framework and the NIST special publication series. The federal government could adopt a workshop-based process that is voluntary, open, and transparent and relies on private sector input and expertise. Deliverables derived from such workshops might outline best practices for data security or other industry developed topics.

4. We have incredible talent and creativity in this country. As a result, individuals and companies continually invent new technologies and methods to address any number of issues, including protection of consumer data. Thus, with the constant evolution of technology, what risks, if any, do you believe are involved in creating a new federal data breach standard?

   An overly prescriptive standard would indeed serve to hamper the benefits of new or evolving technology. However, a new federal data breach standard that is flexible, utilizes a "substantial harm or inconvenience" standard, and is technology neutral would allow for proper management and mitigation of such risks, ensuring that innovative ways to protect consumers continue to be developed.

---

[6] http://www.hsgac.senate.gov/hearings/data-breach-on-the-rise-protecting-personal-information-from-harm

[7] http://www.gao.gov/assets/660/659572.pdf at pp.26-28

FINANCIAL SERVICES ROUNDTABLE

5. Most businesses and many in Congress agree there should be a federal data breach standard, so how do we account for the changing threat landscape and evolving technology when crafting legislation?

   A federal data breach standard should aid consumers, reduce confusion and inefficient resource allocation, and allow for change and evolution in the threat and technology landscape. It should not focus on specific technology or specific mandates, but on the risk of harm to those it seeks to protect. For example, the "Data Security Act of 2014," S. 1927, introduced by Chairman Carper and Senator Blunt, is such a bill. Under its provisions, firms that handle sensitive consumer financial information are required to secure their data. Under the bill, the breach notification process to consumers is based on a reasonable and flexible standard of "substantial harm or inconvenience" to consumers. The measure also permits a reasonable period of time to allow law enforcement to investigate the breach. Moreover, the legislation preempts the existing patchwork of conflicting and often contradictory state data breach law and recognizes financial institutions are already required to comply with existing Gramm-Leach-Bliley Act data security standards and does not add duplicative regulatory burdens. FSR is encouraged by this legislation and looks forward to working with Congress to achieve its objectives.

6. Do you agree with the Federal Trade Commission (FTC) that they should have civil penalty authority as well as Administrative Procedure Act (APA) rule making authority? If yes, why? If no, why not?

   See below.

7. Would greater FTC regulatory and civil penalty authority be an effective incentive for companies to comply with cyber security laws, or conversely, an effective deterrent to companies continuing bad cyber security practices?

   Despite overall and substantial increases in cybersecurity spending, the number of organizations that are victims of targeted and sophisticated attacks perpetrated

FINANCIAL
SERVICES
ROUNDTABLE

by criminal and nation state actors is increasing. If such attacks were effectuated through physical means (rather than cyber means), perpetrators would be the persons or entities that are subject to severe criminal penalties. If the perpetrators were nation state actors, they would be subject to international condemnation and counter measures, potentially involving a military or other national defense response. Cyber criminals should be the focus for increased penalties and consequences. Companies, of course, should comply with cyber security laws and maintain reasonable and appropriate cyber security practices and be held responsible if they do not.

1700 NORTH MOORE STREET
SUITE 2250
ARLINGTON, VA 22209
T (703) 841-2300 F (703) 841-1184
WWW.RILA.ORG

May 30, 2014

The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
344 Dirksen Senate Office Building
Washington, DC 20510

Re: Post-Hearing Questions for the Record of Sandra L. Kennedy following the April 2, 2014 hearing titled "Data Breach on the Rise: Protecting Personal Information from Harm"

Dear Senator Coburn,

On behalf of the Retail Industry Leaders Association (RILA), thank you for the opportunity to testify before the Committee on Homeland Security and Governmental Affairs' April 2, hearing titled "Data Breach on the Rise: Protecting Personal Information from Harm." At the hearing, I testified alongside Governor Tim Pawlenty on the Merchant and Financial Services Cybersecurity Partnership, which is now comprised of over 18 trade associations dedicated to strengthening overall security across the payments ecosystem and bolstering consumer confidence in the payments system. This Partnership is making important strides through constructive dialogue between the merchant and financial services community and we hope to report back to Congress regularly on our progress.

In addition, RILA on May 14, along with several of America's most recognized brands, announced the launch of the Retail Cyber Intelligence Sharing Center (R-CISC), the centerpiece of which is a Retail Information Sharing and Analysis Center (Retail-ISAC). Through the R-CISC, retailers are today sharing cyber threat information among themselves and, via analysts, with public and private stakeholder such as the U.S. Department of Homeland Security (DHS), U.S. Secret Service (USSS) and the Federal Bureau of Investigation (FBI). The R-CISC will also provide advanced training and education and research resources for retailers. These two, private sector-led initiatives show the importance that merchants place on protecting commerce from malicious actors and the security of our customers' personal information.

RILA appreciates the opportunity to respond to your post-hearing questions for the record:

1. Do you think that the federal government is investing enough in investigating and arresting cyber criminals?

The federal government has an important role in protecting commerce and American businesses by deterring cyber criminals through its investigative powers and then the ability to go after, disrupt, shut down and prosecute cyber criminals. One key to this success is the ability of the DHS, USSS and FBI to enter into public-private partnerships with the private sector, such as through the before mentioned Retail-ISAC, in order to share cyber threat information with companies. RILA supports these agencies having the appropriate resources to carry out their missions and the flexibility for them to reassign existing resources based on the changing threat environment.

2. What recommendations would you make for federal agencies to do a better job deterring or stopping cyber crime?

There are many things that the federal government can do to further deter and mitigate cyber crimes. RILA supports an expansive view of cyber security including appropriate deterrences and penalties plus engagement with the private sector to help detect, stop and mitigate cyber crimes. To this end, RILA supports congressional efforts to increase criminal penalties in order to deter cyber crimes on the front end, and then to appropriately bring to justice and punish criminals engaged in cyber attacks. RILA applauds the outreach of federal agencies like the DHS, USSS and FBI to the private sector and encourages the agencies to continue and build upon the strong working relationships they have developed with the private sector.

3. What role, if any, should the government play in encouraging the private sector to strengthen data security?

    a. If there is a role, how can the government both set an example for the private sector in the area of data security and provide businesses the flexibility they need within any federal guidance rather than burdensome regulations?

RILA supports legislation to limit any liability the private sector would have regarding the sharing of cyber threat information with the federal government. Doing so would provide the private sector with the right incentives to share threat information with the federal government without fear that information shared in good faith with the federal government could somehow be used against the entity that shared the information with the federal government. Furthermore, appropriate protections are needed so that threat information shared with the federal government is not subject to Freedom of Information Act (FOIA) requests that could unnecessarily damage private sector entities who are engaged in sharing information with the government in good faith.

4. We have incredible talent and creativity in this country. As a result, individuals and companies continually invent new technologies and methods to address any number of issues, including protection of consumer data. Thus, with the constant evolution of technology, what risks, if any, do you believe are involved in creating a new federal data breach standard?

RILA companies promote data security through the use of administrative and technical safeguards that are proportional to risk and adjust these safeguards as technologies and

risks change. The danger in creating a new federal breach standard that includes a data security standard is that it would not allow for the necessary flexibility retailers need to account for the evolution of technology.

5. Most businesses and many in Congress agree there should be a federal data breach standard, so how do we account for the changing threat landscape and evolving technology when crafting legislation?

   With the ever changing developments in technology, industry is best positioned to adjust on a real time basis. When crafting legislation, Congress should take into account the practical realities retailers face in notifying customers and the proportional risks to harm.

6. Do you agree with the Federal Trade Commission (FTC) that they should have civil penalty authority as well as Administrative Procedure Act (APA) rule making authority? If yes, why? If no, why not?

   While we agree it is understandable for the FTC to have civil penalty authority when enforcing provisions, appropriate caps and other safe guards should be put into place in order to prevent potential overreach.

7. Would greater FTC regulatory and civil penalty authority be an effective incentive for companies to comply with cyber security laws, or conversely, an effective deterrent to companies continuing bad cyber security practices?

   While we agree it is understandable for the FTC to have civil penalty authority, we do not believe that giving the FTC such authority would provide incentive for retailers to comply with laws. Instead, it is something retailers do on a daily basis because it what our customers expect and deserve.

In closing, RILA appreciates the opportunity to provide written responses to your post-hearing questions for the record. If you have any further questions about any of this, please contact RILA's executive vice president for government affairs, Bill Hughes, by phone at (703) 600-2012 or by email at bill.hughes@rila.org.

Sincerely,

Sandra L. Kennedy
President

Post-Hearing Questions for the Record
Submitted to Tiffany O. Jones
From Senator Tom Coburn

"Data Breach on the Rise: Protecting Personal Information from Harm"
April 2, 2014

1. According to the GAO, the number of security incidents in government agencies involving Personally Identifiable Information (PII) for fiscal years 2009 through 2013 increased over 140 percent. Given your experience and knowledge about cyber security threats, do you think that federal agencies' networks are secure?

2. Do you think that the federal government is investing enough in investigating and arresting cyber criminals? Or working to disrupt the international criminal networks that you discussed in your testimony?

3. What recommendations would you make for federal agencies to do a better job deterring or stopping cyber crime?

4. What role, if any, should the government play in encouraging the private sector to strengthen data security?

    a. If there is a role, how can the government both set an example for the private sector in the area of data security and provide businesses the flexibility they need within any federal guidance rather than burdensome regulations?

Responses to these Questions for the Record were not received at time of printing.

○