S. Hrg. 111–1103

CYBER SECURITY—2010

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JUNE 15, 2010
PROTECTING CYBERSPACE AS A NATIONAL ASSET: COMPREHENSIVE LEGISLATION FOR THE 21ST CENTURY

NOVEMBER 17, 2010
SECURING CRITICAL INFRASTRUCTURE IN THE AGE OF STUXNET

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 PRINTING OFFICE
58–034 PDF WASHINGTON : 2011

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
ROLAND W. BURRIS, Illinois
EDWARD E. KAUFMAN, Delaware *
CHRISTOPHER A. COONS, Delaware *

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts
JOHN MCCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina

Michael L. Alexander, *Staff Director*
Deborah P. Parkinson, *Senior Professional Staff Member*
Adam R, Sedgewick, *Professional Staff Member*
Brandon L. Milhorn, *Minority Staff Director and Chief Counsel*
Robert L. Strayer, *Minority Director of Homeland Security Affairs*
Devin F. O'Brien, *Minority Professional Staff Member*
Trina Driessnack Tyrer, *Chief Clerk*
Patricia R. Hogan, *Publications Clerk and GPO Detailee*
Laura W. Kilbride, *Hearing Clerk*

* Senator Coons replaced Senator Kaufman on the Committee on November 15, 2010.

CONTENTS

WITNESSES

TUESDAY, JUNE 15, 2010

WEDNESDAY, NOVEMBER 17, 2010

ALPHABETICAL LIST OF WITNESSES

APPENDIX

PROTECTING CYBERSPACE AS A NATIONAL ASSET: COMPREHENSIVE LEGISLATION FOR THE 21ST CENTURY

TUESDAY, JUNE 15, 2010

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

The Committee met, pursuant to notice, at 2:59 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, Pryor, Burris, Collins, and McCain.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good afternoon and thanks for being here today. We are going to take a look at legislation Senators Collins, Carper, and I introduced last week, the Protecting Cyberspace as a National Asset Act. It provides a comprehensive framework to modernize, strengthen, and coordinate our cyber defenses across civilian Federal networks and the networks of the most vital privately owned critical infrastructure, including some real basics of American life: Our electric grid, financial systems, and our telecommunications networks.

Today we are going to hear from the top cyber security official at the Department of Homeland Security (DHS), which, of course, has a critical role to play in protecting our cyber assets; and we are also going to hear from security and industry experts. We have, in preparing this legislation, consulted extensively with members of the Administration, people in the private sector, and privacy groups as well.

In the 40 years since the Internet was created, it has developed into a necessity of modern life, a source of remarkable information and entertainment and commerce. But as we also have come to know, it is a target of constant attack and exploitation. We now have a responsibility to bring the public and private sectors together to secure the Internet, cyberspace, and to secure it well. And we believe that our bill would do just that.

The idea of cyber crime is not really totally new to the American people. We all know about identity theft and about emails from a foreign prince, doctor, or government official who desperately needs more money, needs to move it out of his or her country, and who will reward you richly—if only you will give them your bank account number, which some people actually do.

Identity theft and financial fraud are serious matters. But, of course, we need, and hope through this bill, to reorient our thinking about the risks inherent in the Internet and cyberspace because today we face much greater risks in cyberspace than crimes like identity theft. A sophisticated attacker could cripple most of our financial system, take down a lot of the electric grid, or cause physical devastation equal to or greater than conventional warfare. The fact is that the threat of cyber attack is among the most serious threats America faces today.

President Obama I think has correctly described our sprawling government and private sector cyber networks as a "strategic national asset." But our efforts to secure those networks and that national asset have been disjointed, understaffed, and underfinanced. So what does our bill do?

First, we need leadership, we need focused and clear leadership, and our bill provides it in the form of a White House Office of Cyberspace Policy that would lead all Federal efforts to defend cyberspace—that is, civilian, defense, and private. The office would be led by a Senate-confirmed director, accountable to the public. We have previously asked, for instance, White House cyber coordinator Howard Schmidt to testify before this Committee, but we have always been turned down, apparently on the grounds of executive privilege. Our legislation would change that by requiring Senate confirmation and thereby making Mr. Schmidt or whoever holds that position subject to the call of Congress and the public.

We also need a stronger agency to defend the dot-gov networks and oversee the defenses of our most critical infrastructure. The Department of Homeland Security Inspector General will issue a report tomorrow critical of many operational elements of the Department's cyber security effort, citing a lack of clear authority as one of the issues that needs to be rectified. Our bill more than addresses these shortcomings by creating a National Center for Cybersecurity and Communications within the Department of Homeland Security which would have new, strong authorities to protect non-defense, public sector, and private sector networks from cyber attack. DHS already has this responsibility through Presidential Directive but, in our opinion, insufficient authority to carry it out.

The sound defense of our cyber networks will only be successful if industry and government work together, so our bill will set up a collaborative process where the best ideas of the private sector and the government would be used to meet a baseline set of security requirements that DHS would enforce for the Nation's most critical infrastructure.

Thanks to some excellent work by our colleague, Senator Carper, our legislation reforms and updates the Federal Information Security Management Act to require continuous monitoring and protection of Federal networks, but do away with the paper-based reporting system that takes up time agencies really otherwise would be using and should be using to protect their networks.

Our legislation also would require the Federal Government to develop and implement a strategy to ensure that the almost $80 billion of information technology products and services that the Federal Government purchases each year are secure and do not provide our adversaries with a back door into our networks. And, of course, if the Federal Government uses that $80 billion of purchasing power to drive security add-ons and innovations in information technology products, it will also be available and presumably bought by the private sector.

Finally, we would give special authority to the President to act in the event of a catastrophic cyber attack that could seriously jeopardize public safety or have disastrous effects on our economy or national security. In those instances, clearly defined in our legislation, the President could direct the National Cybersecurity and Communications Center at DHS to impose emergency measures on a select group of critical infrastructure to preserve those assets and the networks they rely on and protect the American people. These emergency measures would automatically expire within 30 days unless the President ordered an extension. I know there has been some concern and controversy about that provision, and we can speak to it, I hope, in the question-and-answer period. But it is linked with a very important limitation on liability of private entities who take action in response to an order from the government and might otherwise incur liability. But we protect them from that because the action the government is ordering them to take is in the national security or economic interest.

So freedom of expression and freedom to innovate are not inconsistent with greater security in cyberspace and that is exactly what we hope to combine and balance in this legislation.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, I have a very lengthy statement which I would request be inserted in the record in full.[1]

Chairman LIEBERMAN. Without objection.

Senator COLLINS. And I will just summarize my comments.

As the Chairman has pointed out, cyberspace is under increasing assault on all fronts. The cyber threat is real, and the consequences of a major successful national cyber attack could be devastating. As former Director of National Intelligence Michael McConnell warned in February, “If we went to war today, in a cyber war, we would lose.”

We are already under fire. Just this past March, the Senate’s Sergeant at Arms reported that the computer systems of Congress and Executive Branch agencies are now under cyber attack an average of 1.8 billion times a month. Cyber crime already costs our national economy an estimated $8 billion per year.

So it is clear that we must move forward now with an aggressive and comprehensive approach to protect cyberspace as a national asset. The vital legislation that we introduced last week would do just that. It would fortify the government’s efforts to safeguard America’s cyber networks. And it would promote a true public/private partnership to work on national cyber security priorities.

[1] The prepared statement of Senator Collins appears in the Appendix on page 67.

For far too long, our approach to cyber security has been disjointed and uncoordinated. This simply cannot continue. The stakes are too high.

Our bill, as the Chairman has pointed out, would establish an essential point of interagency policy coordination within the White House. This would be the Office of Cyberspace Policy which would be run by a Senate-confirmed director who would advise the President and who would develop a national cyber security strategy.

Let me be clear. We are not talking about creating an unaccountable cyber czar. The Cyber Director would have defined responsibilities and would be accountable to Congress as well as to the President. The Cyber Director would be an adviser, a strategist, not an implementer.

That responsibility, for Federal civilian systems and for the private sector critical infrastructure, would fall to a strong operational and tactical partner at the Department of Homeland Security through a newly created National Center for Cybersecurity and Communications (NCCC). This new cyber center is patterned on the National Counterterrorism Center (NCTC). It would have representatives from various departments and would work on these issues day to day.

The bill, as I mentioned, emphasizes the importance of working with the private sector to improve cyber security across private sector networks.

In cases where owners and operators are responsible for assets whose disruption would cost thousands of lives in mere seconds or multiple billions of dollars, the bill would establish certain risk-based performance requirements to close security gaps.

These requirements, for example, would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted.

But I want to emphasize that the private sector would be able to choose which security measures are implemented to meet the risk-based performance requirements. That model would allow for the continued innovation that is fundamental to the success of the information technology (IT) sector. And as the Chairman has indicated, the bill would also provide limited liability protections to owners and operators of critical infrastructure that comply with the new risk-based performance requirements.

If a cyber attack were imminent or occurring, the bill would authorize the President to undertake emergency measures. But as the Chairman has indicated, we have carefully circumscribed that authority. It is limited in duration and scope. The bill does not authorize any new surveillance authorities or permit the government to “take over” private networks.

The legislation would also take full advantage of the government’s massive purchasing power to help ensure that cyber security is baked into products when they are brought to the marketplace.

And, finally, the bill would improve the recruitment and retention of a qualified Federal IT workforce.

If hackers can bring the nation of Estonia to its knees through cyber attacks, infiltrate a major defense program, and hack into the computers owned and operated by some of the world's most sophisticated private sector experts, we must assume that even more spectacular and potentially devastating attacks lie ahead. We simply cannot wait for a cyber September 11, 2001, before our government takes this threat seriously and acts to protect these critical assets.

Thank you.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

It is the tradition of our Committee that the Chairman and the Ranking Member only make opening statements. It is a selfish system but one that Senator Collins and I both appreciate. [Laughter.]

But on this occasion, since Senator Carper is a cosponsor of our legislation, I would welcome any opening statement that you would have Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you very much, Mr. Chairman. I want to salute you and Senator Collins for bringing this together in a bipartisan—even a tripartisan coalition—on an issue whose time has come. Look around this room. Standing room only. I would suggest that finally at long last we have a strong national focus here in the Senate and in the Administration on taking the steps that we need to take to make sure that our Internet, which has grown more complex by the day, is secure.

For 3 years, I have called for some of the very same reforms that we will talk about today. In fact, I introduced cyber security legislation, I think, last spring in an effort to strengthen our Federal Government—and our Nation—against the kinds of attacks that we have seen seriously disrupt the nations of Estonia, as Senator Collins has mentioned, and Georgia.

One reform that I am especially happy my colleagues have accepted is the creation of a White House office that would be responsible for coordinating the security and resiliency of our Nation's cyberspace. To date, Federal agencies' efforts have been ad hoc; they have been for the most part duplicative. There is an old saying that goes, "the left hand does not know what the right hand is doing." And my hope is that this office will provide the needed strategic direction to more effectively deal with challenges in cyberspace before they become a crisis.

Another reform that I am happy, when it made it into the bill, is the idea that agencies need to leverage their purchasing power to demand that private vendors sell more secure products and services at the front end. For too long agencies have needlessly spent money cleaning up after a cyber attack because the technology was full of security holes. Like a door with no lock, hackers have used security holes that never should have been there in the first place to gain access to our sensitive networks, and this bill changes that.

I also want to commend my colleagues—and our staffs, and I especially want to commend Erik Hopkins, who is sitting right behind me, for the work that he has done on these issues for years. But I commend all who have been involved in reforming the Federal Information Security Management Act of 2002. As we all know, producing a plan that sounds good on paper is not the same as ensuring the plan is effectively implemented. That is why our legislation compels agencies to stop producing the reams of ineffective paperwork they currently do and instead focus their efforts on defending their systems in real time, much as we do in the nuclear power industry.

Last, I want to thank my colleagues for accepting my language to create a nationwide network of cyber challenges to help reduce the gap between the number of so-called cyber warriors that are produced in America and those that are being trained in place like China, North Korea, and Russia. A little bit like a farm system in baseball, these cyber challenges will create a pipeline of talent that can be tapped by government agencies and by private sector companies. If we want America to continue to be dominant in the century to come—and we know we do—we have to invest in the skills of these young people.

In closing, I look forward to working with our Chairman, with Ranking Member Collins, and other colleagues who have an interest in these issues, including Senator McCain to my left, and my colleague, Senator Burris from Illinois, who I know has a strong interest in these issues. My hope is we can bring together a diverse group of stakeholders on all sides of the issue to produce a bipartisan/tripartisan bill that will enhance our Nation's cyber security and be signed by the President before the end of this week—or maybe this month. How about this year? Thank you.

Chairman LIEBERMAN. Thanks, Senator Carper. Thanks to Senator McCain and Senator Burris for being here.

We will go to our first witness, Philip Reitinger, Deputy Under Secretary of the National Protection and Programs Directorate, and Director of the National Cybersecurity Center at the Department of Homeland Security. Mr. Reitinger's coming to the Department is part, I think, of a really full open-throttle attempt to dramatically upgrade the Department's capacity for cyber defense. He has a remarkably diverse background in both the private sector and government, which includes working at both Microsoft and the Department of Justice, though not at the same time.

Mr. REITINGER. Thank you, sir. You left off the Department of Defense as well.

Chairman LIEBERMAN. Sure.

Anyway, Mr. Reitinger, I am glad to see you again, and we welcome your testimony now.

TESTIMONY OF PHILIP REITINGER,[1] DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. REITINGER. Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is indeed an honor to appear before you today to talk about the security of cyberspace and this Committee's Protecting Cyberspace as a National Asset Act.

As you point out Mr. Chairman, the President has described our networks as a strategic national asset. And as the Ranking Member pointed out, those networks are under an increasing threat and increasing risk of harm every day. The attackers range in skill from state-sponsored attackers down to low-level criminal hackers.

[1] The prepared statement of Mr. Reitinger appears in the Appendix on page 72.

And the fundamental insecurity of our ecosystem means not just our information is at risk, but the information infrastructure that provides us critical services is also at risk, as the Committee Members point out: Power, financial services, transportation, and other key parts of our infrastructure. That means it is incumbent upon all of us—across the government, the State, local, tribal, and territorial governments, and the private sector—to treat this as a real national security and homeland security emergency. We must respond to deal with the increasing threat.

The prior Administration began a good start in this space with the Comprehensive National Cybersecurity Initiative, which President Obama furthered with the Cyberspace Policy Review. We, in DHS, are similarly recognizing our responsibility. We are the lead for working to protect Federal civilian systems and working to protect private sector and State, local, tribal, and territorial government systems and helping them to bolster their cyber security.

A key moment happened in February of this year which escaped a lot of people's notice. The Department of Homeland Security released, after interagency review, the first ever Quadrennial Homeland Security Review, which was released, interestingly, on the same day as the Quadrennial Defense Review. And I would urge everyone who has not to read the cyber sections of those two documents because they are parallel. The Department of Defense (DOD) recognizes its increasing need to be involved and treat cyber security as a growing mission set. And the entire homeland security enterprise—and that is broader than just the Department of Homeland Security. It includes the private sector. It includes multiple other government agencies and State, local, tribal, and territorial governments. It treated cyberspace and the security of cyberspace as a top five mission area of that enterprise, on a par with protecting the borders and ensuring domestic security. So we are well on the way towards treating this as a national and homeland security event.

In that line, we have had significant outcomes over the course of the past year that demonstrate our intent to move forward. I am a firm believer that, in government or the private sector, organizations succeed or fail based on the people who are doing the work. If you have the right people, technology does not matter too much. And if you do not have the right people, then technology does not matter too much.

There was a great core of people at the Department of Homeland Security when I arrived, and we have been expanding that as rapidly as possible. During the course of the last fiscal year, fiscal year 2009, we increased the people who do cyber security in the Office of Cybersecurity and Communications from 35 to 118. And in the course of this fiscal year, we are trying to more than double it again.

We are rapidly deploying EINSTEIN 2 on the technical side. We are ahead of schedule. It is deployed and operational at 11 of 19 agencies where it is to be deployed, and at four Internet service providers it is deployed, and in one it is operational. Through those deployments, we are already discovering, apropos of the comments that the Ranking Member made before, more than 278,000 indicators on average of potentially malicious activity per month.

Finally, with regard to FISMA, the Administration is moving rapidly to recognize the criticisms that have been made of that regime in the past. In particular, a key focus in the Administration is moving away from annual paper reports and more towards continuous monitoring. What is the real security situation we are in? And apropos of where this Committee is intending to go, providing the operational responsibility to manage that effort to the Department of Homeland Security.

Turning finally to the bill, I regret I am not able at this time to state an Administration position on the bill which was introduced last week. That said, DHS looks forward greatly to continuing to work with the Committee on strengthening the Department's ability to accomplish its cyber security mission. I particularly welcome this Committee's and the sponsors' support for the DHS mission, its support for allowing DHS' effort to maximize its hiring flexibilities, and the continuing and clear support in the bill for privacy and civil liberties, which we believe are fundamental to cyber security.

With regard to authorities, we believe the continued examination of authorities for both DHS and in emergencies is called for to see what can be done under existing authorities and what changes may be necessary.

Finally, I would state that with regard to organization, it is the Department of Homeland Security's view that our preference is to keep physical and cyber security tightly co-joined. We believe that it will enable us to work more effectively with the private sector to manage risk, give us—to the extent one wants to influence the private sector, which is important—more levers to pull, and allow us to continue to work with the private sector in an all-hazards way on instant response.

Mr. Chairman, Ranking Member Collins, Members of the Committee, thank you again for the opportunity to testify, and I would be more than pleased to answer any questions you may have.

Chairman LIEBERMAN. Thanks, Mr. Reitinger. I appreciate the fact that though there is not an official position of the Administration on the bill, you are giving your own welcome and warm response, particularly of the role given to the Department. Is that right?

Mr. REITINGER. We certainly welcome the support for the DHS mission space, sir, and the clear delineation of roles and responsibilities, absolutely.

Chairman LIEBERMAN. Fine. Let me just start out, and we will do 7-minute rounds. Let me ask first, if somebody comes up to you and says, "Is all this business about cyber security for real? In other words, are we really under threat from non-state actors, other states, or terrorist groups? Can they really do as much damage as a conventional attack?" What do you say?

Mr. REITINGER. Sir, the threat is clearly real. I often say—in fact, I said yesterday when I was in Miami at the Forum of Instant Response Teams event—that if you really want to secure your computer, it is best to turn it off, disconnect it from the Internet, and if you really want to be secure, do not allow any person to get near it, open up the cover, pull out the hard drive, and hit it with a hammer until it no longer can be read.

The current state of the technology simply does not allow for foolproof security. Instead, we are in risk management. And right now we have a long way to go to be able to as effectively manage risk as we need to.

We depend on these companies not just to see a silly video on the Internet or even to write a document to pass up the chain of command. We depend on them for power, for food, and for transportation. Those systems are insecure in many ways, and we simply do not live in a sustainable environment right now. The system is fundamentally insecure and needs to change.

Chairman LIEBERMAN. So the capacity to attack in cyberspace or intrude or exploit is, therefore, much greater than the capacity to defend against such attacks?

Mr. REITINGER. Yes, sir.

Chairman LIEBERMAN. I do not want to carry you too far into a parade of horribles, but is it really possible that a cyber attack on, for instance, private infrastructure could cause damage comparable to a conventional military attack on our homeland?

Mr. REITINGER. Sir, I think it is hard to know the full scope of damage. I think it is possible damage. It is certainly likely that significant economic damage could be undertaken. If a cyber attack, for example, destabilized people's trust in the financial system, one would see untold economic costs to this country. And physical attacks are possible, and we need to advance the state of science and the art of the possible to know what the full scope of risk is. In any event, we need to prepare now as if it were possible.

Chairman LIEBERMAN. Yes. Let us talk about what we can do to better defend, and let me ask you to compare or respond to some alternative suggestions to the one that we have included in our bill. There are proposals moving around different sections of Congress that would have the Department of Defense or the intelligence community take the lead on protecting the Federal civilian networks. Obviously, DOD is responsible for the defense networks now, and, of course, our bill respects that totally. But there are these proposals saying DOD or the intelligence community should take the lead in protecting Federal civilian networks as well as those of private critical infrastructure.

From your point of view, what is the argument for why the Department of Homeland Security, as opposed to those other agencies, should have that responsibility?

Mr. REITINGER. Sir, the Department of Homeland Security has been given the responsibility for helping to protect the dot-gov, the civilian government systems, and working with the private sector under both the prior Administration and this Administration. It is what we do, it is our role, and that is appropriate.

Every agency brings its own capabilities to bear, and I by no means wish to undercut the key role of the Department of Defense or the expertise it brings to bear. This Nation has spent significant dollars over a long period of time to develop technical capabilities in the Department of Defense, which the Department of Homeland Security can and does leverage in its role of working with the private sector and protecting civilian government systems. We leverage and synchronize the capabilities of the Department of Defense in significant amounts of the work that we do, and we coordinate with them fully and partner with them across the Federal Government enterprise.

DHS has in its own space developed its own capabilities. We have built as a part of the National Infrastructure Protection Plan the partnership framework under which we work with the private sector. We have built the capability to deploy teams to work in particular private sector environments and provide support. We have built the ability to help control systems' vendors and those who deploy control systems to respond to cyber events and to help secure their systems.

By working together and each playing our positions and bringing our capabilities to bear, one team, one fight, we can be most effective across government.

Chairman LIEBERMAN. Do you have particular concerns, for instance, about DOD or the intelligence community taking over nondefense civilian government networks or private infrastructure? I know some people have been concerned about privacy or civil liberties in that case.

Mr. REITINGER. Sir, I believe both General Alexander, the Director of the National Security Agency (NSA), and now the head of Cyber Command, and other individuals from DOD have been clear over time that protection of the civilian government space and working with the private sector is the mission space of the Department of Homeland Security, that they are intent to support. And I believe they will do that, and we will work effectively together.

Chairman LIEBERMAN. Let me ask you one last question. I believe that DHS is the right place for this authority to be. I am also encouraged because I think you bring a lot to the position you are in now. Personnel are really key in this, and our bill respects that by creating flexibility in hiring for the new section that we are creating and beefing up in DHS. So I want to ask you to respond to those suggestions in our bill and whether you think they are important and whether you think they are adequate.

Mr. REITINGER. Sir, I cannot comment on the specific provisions in the bill because the Administration is still reviewing it, but I can say that hiring flexibility is very important to the Department of Homeland Security, in particular in the cyber security area.

Chairman LIEBERMAN. And this really means being able to pay people more than the normal pay scale in Federal service because that is what you have to do to get the best people. Is that right?

Mr. REITINGER. It means paying more in particular cases. It means having the flexibilities to be able to hire people rapidly. As you can imagine, there are far too few cyber security experts in our country. And, indeed, one of the long-term things we need to accomplish is enhancing our educational system so that there are more such people available to go to the private sector and the government.

But now we are in a space where we are competing substantially with private industry that can pay a lot more. We succeed by, first of all, giving those individuals a chance to really make a difference, to tell them that we have a critical mission, and you as a patriot can help your country; second, by giving them the ability and capability to actually make a difference; and, third, by asking them not to make too many sacrifices. We are very clear. If you come to work for the government, indeed, any part of the government, you are going to make a sacrifice if you are in cyber security because you are not going to make what you could in the private sector. But if we can bring them on more rapidly and pay them something comparable to what they would get in the private sector, they will do that to help protect their country.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Thank you.

I was struck in your written testimony by the Administration's continued reliance on Section 706 of the Communications Act as the basis for emergency authority in the event of a cyber attack. In fact, while your testimony is a little bit unclear on this point, you seem to be opposing the attempt that we have in our bill to lay out the authorities of the President, and instead you are pointing back to this Act.

I would point out that authority was passed in January 1942. It was passed a month after the attack by the Japanese on Pearl Harbor—obviously, a very different time and long before the Internet was even conceived of.

In light of the current nature of our communications infrastructure, the Communications Act grants very broad authority to the President, but it is authority that can only be exercised when a certain threshold is met, and that is the state of war or the threat of war. It is wholly lacking in the kinds of flexibility to respond to a serious attack targeting some of our most critical infrastructure that may fall below that threshold.

Is it clear, based on legal research DHS has done, the opinions of the Federal Communications Commission, or some court decision, that the authority of Section 706 could be used to respond to an attack on our critical infrastructure that does not rise to the level of the state of war or the threat of war?

Mr. REITINGER. So, ma'am, let me first begin by saying while Section 706 is one authority and, as you point out, a hoary one that inures to the President of the United States, there are other legal authorities the President could bring to bear. Your point I think is well taken, though, that those authorities, for the most part, are older or not specifically designed for this case.

That said, the Administration's position is to prefer to see if those authorities could be aligned in a way that would allow the need to be met, and if movement goes forward, to do so in a way that would be minimally disruptive. I would say that there are a lot of legal questions that have not been answered. The Cyberspace Policy Review identified a significant number of them. We and the Administration, I think, would be happy to work with this Committee to make sure that the authorities that are necessary to meet the coming need are present to the Department of Homeland Security or the President of the United States in an appropriate emergency.

Senator COLLINS. Well, shouldn't we be carefully defining what authority the President has? Our bill has far more targeted authority to respond to a cyber emergency, but that authority is limited both in duration and scope. It requires notice to Congress. It does not authorize the President to take over networks. It allows the private sector to propose alternative means of achieving the goal.

Shouldn't we be spelling out exactly what the President's authority is short of a state of war?

Mr. REITINGER. Ma'am, I apologize that I cannot take a position on the bill at this time, but I do appreciate the effort that the Committee made to tailor the authorities so they are focused on the expected need.

Senator COLLINS. I will take that as a yes. [Laughter.]

I would say—and I am not trying to put you in an uncomfortable spot, but as you know, we have been working with the Department on this issue for more than a year, and I just do not understand why the Department is not further along in its thinking on what should be done. And that is one reason why the three of us proceeded with a bill. We cannot wait. Those hackers are not waiting. The 1.8 billion attacks per month are occurring now.

So I guess I would ask you to take a look at those provisions of the bill. They are carefully circumscribed and yet aggressive enough, and they reflect the reality. Relying on a law passed in World War II is just foolhardy. It is out of date.

Let me switch to another issue. Tomorrow the DHS Inspector General will release a report that the Chairman referred to that will say that the U.S. Computer Emergency Readiness Team (US-CERT) program, which is charged with monitoring the security of civilian cyber networks, does not have the enforcement authority that it needs to ensure that agencies comply with its recommendations and mitigation guidance. It also notes that US-CERT does not have the authority to compel agencies to deploy technology for determining in real time if a cyber attack is taking place.

Our bill would correct those problems. We would enhance the authorities of US-CERT and create a stronger cyber center within DHS, including providing the center with the authority to enforce compliance with its cyber security directives.

Do you agree that the Department needs additional authorities to enforce security policies for civilian Federal networks?

Mr. REITINGER. Ma'am, as your question points out, the Department does have broad authority within the civilian government space to set requirements for other agencies to meet. The Department does not have direct enforcement authority over those departments and agencies, which has raised issues in particular cases, for example, in Conficker, where we had difficulty in obtaining responses regarding the scope of the issue for different departments and agencies.

So we have, I think, strong authorities right now in terms of setting requirements. In terms of enforcement, we have the commitment, I think, from both the cyber security coordinator at the White House and the Office of Management and Budget (OMB) to work with us when agencies have difficulty in responding to our requirements. And they may do so for a number of valid reasons, including they themselves have limited resources and ability to respond because they are, in fact, just barely able to keep the attackers at bay. We will work through the White House in order to make sure that there is as full compliance as possible.

Senator COLLINS. Well, it is evident to me that the Department needs more teeth in its directives, or agencies are going to feel free to ignore them, and that is one of the problems we are trying to rectify. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

I just want to endorse both lines of the Senator's questioning, but particularly the first one about the need for a clear statement of the authority of the President in the case of a national emergency regarding cyber networks, because I think the old Telecommunications Act does not do it. It is at best unclear. And, of course, in a crisis I would hate to have lawyers arguing in front of the President about what the right thing to do is as we are about to be attacked in cyberspace. If there is an attack on our electric grid, I do not see in the old telecommunications law the power in the President, or anybody, for instance, to order that a patch be put on some part of the grid to protect it. So I hope you will take a good look at that and agree when you do that we need new clearly stated authority.

Senator Carper.

Senator CARPER. Thanks, Mr. Chairman.

Mr. Reitinger, welcome. Good to see you. Thank you for your testimony and for your service on many fronts.

You may have said this and I missed it, but I can appreciate why the Administration may not have a position on this legislation today. Did you say when you expect to have that kind of position—or establish a position?

You said later or tomorrow? Is that what you said?

Mr. REITINGER. Predictions about the vagaries of the interagency process are beyond my cognitive skills. I would hesitate to venture a guess, but it is of importance to us and the Administration, and we will be focusing on the bill.

Senator CARPER. All right. The old saying goes something like this: "The best defense is a good offense." And we are talking a lot here today and have been talking for several years about how to play good defense. Talk to us about how we might play better offense.

Mr. REITINGER. Sir, offense is mostly outside my realm of responsibility now. I am in a part of the U.S. Government that plays defense.

What I can say is that particularly with regard—if you count law enforcement investigations as part of offense, we do need to have the right deterrence structure, and so we partner very closely with our friends in the Federal Bureau of Investigation (FBI) and the Secret Service to make sure that we bring the necessary capabilities to bear, that we liaise with them so that they are able to work as a part of a cross-government partnership. But we are, within the parts of DHS that report to me, very focused on playing defense, and that is our area of responsibility.

Senator CARPER. Whose job is it to play offense on our team?

Mr. REITINGER. Well, generally it would depend on what the role would be, sir. I am not necessarily in a position to say who does what different pieces, but the overall responsibilities roll up to the White House.

Senator CARPER. All right. A month or so ago, I believe, we met with you and some of your colleagues to discuss the role of the Department in securing our Nation from cyber attacks. In addition, we discussed whether or not the Department needed to be internally reorganized to more effectively prevent and defend against both physical and against cyber attacks. In your written testimony today, you mentioned that you believe the Department should have an all-hazards approach to security. I have a couple of questions that flow from that.

Do you believe our bill reorganizes the Department of Homeland Security in a way to better handle both cyber and physical attacks? And a second half to the question is: Do you think there will be any unintended consequences by splitting cyber and physical security responsibilities into two entities?

Mr. REITINGER. Sir, I would say that I appreciate the effort the Committee made to ensure coordination between physical and cyber by including a deputy for physical infrastructure protection within the NCCC, if I could use that acronym. However, I do believe that DHS will be more effective if we keep physical infrastructure protection and cyber infrastructure protection co-joined.

We are, as we move forward, increasingly finding ways that those sub-components, can work together even more effectively. For example, when we do assessment work for our critical infrastructure facilities, doing physical and cyber infrastructure assessments at the same time by working to build out our all-hazards response capability. We have already collocated our cyber watch centers in the National Cybersecurity and Communications Integration Center, and we are thinking through the extent to which we should better merge those with our National Infrastructure Coordinating Center, which coordinates a lot of physical response activities, because the private sector speaks the language of all hazards. They worry about risk, as a telecommunications company would say, whether it is from a cyber attack or a backhoe.

We, in government, need to step to that and speak their same language. If we want to influence how they behave in an all-hazards way, in a risk-based way, and if something bad happens, physical or cyber, to be able to address it seamlessly.

Senator CARPER. All right. I have one more question. I chair a subcommittee of the Committee on Environment and Public Works that deals with nuclear safety. We have about 104 nuclear power plants, as you may know, and the nuclear industry and the Nuclear Regulatory Commission (NRC) which regulates that industry use force-on-force exercises where good guys act like bad guys and they test whether or not our 104 nuclear power plants are prepared for an assault from a force of truly bad guys. This is also known as offense informing the defense.

It is widely recognized that the National Security Agency has developed the most sophisticated capabilities in the world to exploit other groups' sensitive networks. This knowledge and experience of the offense has allowed the NSA to develop better defenses to protect their own systems and networks. I included provisions in our cyber bill to help the Department of Homeland Security also to do this.

What is the Department doing now to better enhance the defenses of the Federal Government using the NSA model?

Mr. REITINGER. I guess I would answer that in two parts, sir. To begin with, we rely on NSA technical assistance and we leverage their capabilities. So we look strongly at the capabilities they have developed as we move forward with technical approaches to decide what the best approach to protecting dot-gov is. That is the general answer.

The more specific answer is with regard to the activities you talk about, such as red teaming and blue teaming. I would say we have yet to fully develop the capability to be able to execute on that. The ability to do that sort of red teaming and blue teaming activity is included in our fiscal year 2011 budget, and we will fully coordinate with and rely on the capabilities and the expertise that NSA has developed in doing that.

I have specifically spoken to Tony Sager at NSA who is a nationwide expert in the cyber defense part of NSA, and we will fully rely on what they can bring to bear as we develop our own capabilities to execute a similar strategy within the dot-gov space.

Senator CARPER. My time has expired. Thank you very much.

Mr. REITINGER. Thank you.

Chairman LIEBERMAN. Thank you, Senator Carper. Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman, and I thank you and Senator Collins for your hard work on this comprehensive legislation.

Mr. Reitinger, besides the fact that you work there, why should the Department of Homeland Security be the lead agency?

Mr. REITINGER. For defending government and the private sector? Because we are ideally positioned to do it, sir, because it is a part of homeland security, because we can and will partner with the Department of Defense and other key government agencies to bring all national capabilities to bear, including leveraging the capabilities of the Department of Defense, and because we can provide the transparency and accountability that the American people expect in full partnership with other government agencies.

Senator MCCAIN. What does "full partnership" mean, Mr. Reitinger? Somebody has to lead. "Full partnership" means equality, so let us be careful with our verbiage here. Do you think that we have already been the victim of cyber attacks?

Mr. REITINGER. Yes, sir.

Senator MCCAIN. Do you think we are basically in a cyber war right now?

Mr. REITINGER. Sir, I hesitate to use——

Senator MCCAIN. Cyber conflict?

Mr. REITINGER. Sir, we live in a very threatening cyber environment, yes.

Senator MCCAIN. Who is our greatest attacker, most significant attackers?

Mr. REITINGER. Sir, I would prefer to address that more in closed session, but the scope of attackers runs the spectrum from low-level criminal hackers to the most significant adversaries.

Senator MCCAIN. Russia mobilized a very effective cyber attack against Georgia prior to their invasion by conventional forces. Isn't that correct?

Mr. REITINGER. Sir, there was a significant attack against Georgia. Yes, sir.

Senator MCCAIN. And there has been one against Estonia?

Mr. REITINGER. Estonia suffered a significant attack as well.

Senator MCCAIN. And do we know where that came from, from Russia?

Mr. REITINGER. Sir, I am not prepared to attribute that activity on the record.

Senator MCCAIN. Every media in America is, but you cannot.

Mr. REITINGER. Sir, from our perspective, if I could, sir—and I do not mean to be flippant.

Senator MCCAIN. You are not flippant. You are just not forthcoming.

Mr. REITINGER. I apologize, sir.

Senator MCCAIN. That is all right.

Mr. REITINGER. For us in the Department of Homeland Security and for the people that work for me and with me, we approach these events to cover the spectrum of threats. Certainly the attackers run the gamut from Nation states down to criminal hackers and everything in between—organized criminal groups, organized hacker groups—and we need to bring the right protections to bear to enable us to protect against that full spectrum of threats.

And "full partnership," sir means that we are involved in helping to secure government systems. We do not secure the Department of Defense systems or the intelligence community systems. We do not engage in international cyber conflict. We instead work to fulfill our role and enable entities like the Department of Defense to fulfill theirs. And I think that the Department of Defense would say the same thing about us.

Senator MCCAIN. But obviously the Department of Defense would be probably the area we would most want to protect over any other if we had to prioritize.

Mr. REITINGER. The Department of Defense is a key entity to protect, sir, as are other parts of government and key parts of the private sector that provide essential services, such as the power grid and our financial services system.

Senator MCCAIN. Well, Mr. Chairman, I notice that there are different bills going through different committees—the Senate Armed Services Committee, the House Armed Services Committee, the Commerce Committee, and the Foreign Relations Committee. At some point I would suggest we are going to have to consolidate or discuss or come to some kind of agreement rather than have a number of competing pieces of legislation here.

I have to say, after the Department of Homeland Security's handling of the Christmas bomber and other activities, I am not confident that DHS, at this particular time, is the proper bureaucracy to work in partnership with the Department of Defense.

I thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator McCain. We will continue to try to convince you that DHS can do it, and Senator Collins and I agree that—we hate to attribute blame, but the State Department made the more consequential errors, unfortunately, leading up to the Christmas Day bombing. So we will continue to work on that.

Senator MCCAIN. Thank you, and I thank the witness.

Chairman LIEBERMAN. Incidentally, you are absolutely right. There are bills on this subject that are moving through various committees. There is none quite—well, I should not say that. Senator Snowe and Senator Rockefeller have introduced a bill in the Commerce Committee that is comprehensive. We think ours is more comprehensive, but the other bills in the Armed Services and Judiciary Committees go to points of this. I know the Majority Leader intends for there to be a blending of these bills into one bill that comes to the floor.

Senator Burris.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS. Thank you, Mr. Chairman.

Mr. Reitinger, I understand that you cannot comment on the legislation, and some of the questions that Senator McCain just raised or some of the points that are going through my mind in terms of the current status. What is the current status of our protection of cyber piracy within our financial system, our military system,and our power grid? What is your current assessment of the cyber activity today?

Mr. REITINGER. Sir, I would say, although this may be an unsatisfying answer, it varies greatly. Through all the infrastructures you mentioned and government agencies you mentioned, the level of defenses vary considerably. There are parts of the government, such as the Department of Defense and other agencies, that are very well protected. There are other agencies that have more areas of growth.

There are sectors and components of sectors in places like the financial sector or the energy sector that do very well and others that have a lot of work to do. That is, I think, one of the concerns because sometimes cyber security is only as strong as its weakest link and the interdependencies are very great.

Senator BURRIS. Do we currently have authority to protect our financial system? Can Homeland Security deal with the hundreds of billions of dollars that is being stolen from the financial arena today which they do not even report?

Mr. REITINGER. Sir, there are certainly authorities in that space. There are a number of law enforcement authorities that would allow investigation and prosecution of those who commit——

Senator BURRIS. Does Homeland Security have any input in that today?

Mr. REITINGER. Yes, through the Secret Service, sir.

Senator BURRIS. So the Secret Service has the cyber authority.

Mr. REITINGER. The Secret Service has the investigative authority along with the FBI for those types of crimes, yes, sir.

Senator BURRIS. So you do not have that authority?

Mr. REITINGER. Not within the parts of Homeland Security that report up to me, no, sir.

Senator BURRIS. OK.

Mr. REITINGER. Our authority, sir, with regard to the private sector is that of coordination. We can raise awareness. We have capabilities that could help them.

Senator BURRIS. I do not give too much credence to all our TV programs, but "60 Minutes" just the other day ran a segment on cyber terrorism. Are you familiar with that information that came out to the public recently?

Mr. REITINGER. I am familiar with some of the things the program said, sir.

Senator BURRIS. Sir, are you familiar with the "60 Minutes" program? It is a simple yes or no answer.

Mr. REITINGER. Yes, sir, I am familiar with "60 Minutes" generally.

Senator BURRIS. No, the program.

Mr. REITINGER. No, sir, I am not.

Senator BURRIS. Thank you. It took us 2 seconds to say no. Do not be so defensive.

What we have here, Mr. Reitinger, is a concern of public confidence in our system, and what I would assume is that there are entities out there that are seeking to enrich themselves, but also to break the confidence of the public. So there is a public factor to this if Americans feel that we are not secure. I want to ask you whether or not you think we can protect our systems?

Mr. REITINGER. Completely, sir? No. Substantially, we can take action and respond to attacks when they occur, and we are continuing to enhance our ability to do that. But completely protect and prevent——

Senator BURRIS. What is your timetable on that? Because as I understand the "60 Minutes" report, we are losing data every day. They are right now from this report sitting in the Pentagon on our military computers, little types of information that can now direct those systems that we might not even be able to control. Are we dealing with anything like that? Are you familiar?

Mr. REITINGER. Sir, we are moving forward very rapidly. As I mentioned, we are rolling out the EINSTEIN 2 intrusion detection system. That is deployed to 12 of 19 departments and agencies where it will be deployed, and it will be deployed to all 19, we forecast, by the end of the fiscal year, so by the end of September.

In terms of when compromises take place, pursuant to the President's Cyberspace Policy Review, we are developing a national cyber instant response plan process. That is nearing substantial completion. It will be vetted, and it is going to be tested in September of this year. There are other efforts on a longer timeline and other efforts on a short timeline. So we have significant efforts going across the ecosystem.

For example, you talk about the financial services sector, sir. We are right now piloting an activity in partnership with the Department of Defense and the financial services sector through their Information Sharing and Analysis Center, a body they voluntarily formed, where we share threat information with them now on an unclassified level, going forward on a classified level, where they also share information through the financial services Information Sharing and Analysis Center back with us and each other. So that is building a much better understanding of the threat and what entities need to do to respond to it in that sector.

So there are a number of different efforts we are moving, sir.

Senator BURRIS. I just wonder what we are doing to other countries with our system. I just hope that we also have cyber piracy going on to counteract the cyber piracy that is coming against us. And in your layman's opinion—not your professional opinion—would you say that we have some going on?

Mr. REITINGER. Sir, I cannot comment on that. I apologize.

Senator BURRIS. Thank you, Mr. Chairman. I have to end my questioning.

Chairman LIEBERMAN. Thanks, Senator Burris.

If I may offer an opinion, not being a member of the Administration, my own impression, let us put it that way, is that the U.S. Government has a very well developed cyber offensive capacity if it becomes necessary to use that to protect our security, and that should be comforting to the American people. But I do want to come back and underline something Secretary Reitinger said, which is the capacity of those who would attack us is much greater right now than our capacity to defend against those attacks. And we are closing that gap. But this legislation and the resources that the Administration is putting behind this are aimed at eliminating the gap. So it is with that intention that we go forward.

I want to indicate—you may have heard this already—that Senator Collins and I are going to take this bill to a Committee markup next week, so we really want to move this out. And in that regard, I urge you to do everything you can—although I know a lot of this ultimately will be in OMB—to have an Administration position developed on this legislation and the other legislation.

Senator Harry Reid has been very clear, at least to me, that he really wants to pass a cyber security act this year, so I hope you will be authorized soon to get more explicitly into the debate.

Mr. REITINGER. Thank you, sir.

Chairman LIEBERMAN. Thank you. Thanks for your testimony.

We will call the second panel, beginning with Fran Townsend. It must give you real pleasure to be out of Federal service as you hear me talk about the need for approval from OMB.

Ms. TOWNSEND. Exactly.

Chairman LIEBERMAN. On the second panel, we are very pleased to begin with Fran Townsend while you are getting seated. She is now the Chairwoman of the Board of the Intelligence and National Security Alliance, a former Homeland Security Advisor to President George W. Bush, and a star of screen, if not yet stage. Welcome.

TESTIMONY OF FRANCES FRAGOS TOWNSEND,[1] CHAIRWOMAN OF THE BOARD, INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Ms. TOWNSEND. Well, thank you, Mr. Chairman, for that introduction. It is really a privilege to be back with you and Ranking Member Senator Collins. Thank you very much for your invitation to testify at this hearing and to offer my thoughts on the Protecting Cyberspace as a National Asset Act of 2010.

I am here today in my role, as you noted, as Chairwoman of the Board of the Intelligence and National Security Alliance (INSA). It is a premier not-for-profit private sector professional organization

[1] The prepared statement of Ms. Townsend appears in the Appendix on page 80.

providing a structure and interactive forum for thought leadership, the sharing of ideas, and networking within the intelligence and national security communities. INSA has over 100 corporate members as well as several hundred individual members who are leaders within the government, private sector, and academia. And as I think you are aware, INSA prepared and submitted my statement for the record while I was out of the country. I arrived home yesterday. So I will also add a few of my personal observations before I close.

Through its Cyber Security Council, INSA has emphasized the importance of creating a strong public-private partnerships that can provide meaningful recommendations to address the national and economic security threat today. I would like to specifically speak to the importance of establishing a public-private partnership to promote national cyber security priorities, strengthen and clarify authorities regarding the protection of Federal civilian systems, and improve national cyber security defenses.

Collective national cyber security can only be effectively addressed through a partnership approach between the government and private industry. While the government has the legal authority required to organize markets, enforce laws, and protect citizens' privacy and property, the vast majority of cyberspace infrastructure, as you all noted, is privately owned and operated. And as a result, industry is where most of the expertise in the fields of IT and cyber security reside. Because of this, a partnership is really the only way forward.

INSA's Cyber Security Council studied several different models of public-private partnerships during the preparation and research for its November 2009 report entitled "Addressing Cyber Security Through Public-Private Partnership." Historically, effective public-private partnerships have inclusive private sector membership, unified in the pursuit of common goals, a single responsible and accountable government partner organization, and clearly delineated roles for both public and private entities. We are very pleased to see these concerns and this organizational structure reflected in the legislation we are here discussing today. This bill not only establishes a clearly responsible center for the problem, but requires a private sector advisory council to advise the center on their actions' effects on industry.

Assuring that private sector concerns are heard within government is an important first step to the creation of a public-private partnership, but this alone is not sufficient to guarantee success. INSA's Cyber Security Council has identified three additional components, specific to a public-private partnership on cyber security, which would be required for a successful effort: First, a flexible or incentivized approach to regulation; second, robust information sharing and cooperation; and, last, communication on standards and best practices.

In the interest of time, I will not go through each of those and would ask that you refer to my statement for the record which we earlier submitted.

In terms of my personal observations, all of which are addressed by the legislation, but I think based on my own experience, knowing that this will go to a negotiated process in the Senate, I think it is worth underscoring their importance.

I support the creation of a National Center for Cybersecurity within DHS because of their abilities uniquely to address privacy and civil liberties concerns that affect all Americans. Because of their necessary reliance on the Internet for our personal lives, I think that their ability to address those concerns will be critically important in ensuring public support for such a center. But I want to be clear that in my judgment to be effective, wherever such a center is, in fact, housed, it must have several key ingredients to be successful. And, again, these are all contemplated by your bill.

First, interagency and cross-government capability, both vertical down to the State and local level and up to the Federal Government, and across the Federal Government as well as including the private sector. As Senator Collins noted, NCTC, which is effectively in the Office of the Director of National Intelligence, is the best analogy, and the NCTC does report to the White House. And that is a model that ought to be preserved as stated in the bill.

Second, budget and enforcement authority is really necessary. Money to implement any steps or affect Federal agency spending is a necessity, and authority to punish or call out across Federal agencies those departments that fail to meet basic standards is also a necessity.

Personnel authority, adequate ability to hire and fire, is necessary to ensure a competent and experienced staff of professionals. While the current bill, as I noted, does contemplate these important steps, I worry about language such as develop a plan, coordinate, recommend, assess, and consult.

I had the privilege of working with the Chairman and Ranking Member on the Intelligence Reform and Prevention of Terror Act, and while we were well intentioned and I believe that was a good and necessary bill, it is the bill which established the Director of National Intelligence. And while this was an important and necessary step, it has been referred to recently as “organized to fail.” I think what those critics would say is that the position lacks some of the necessary authorities that this bill contemplates and would most respectfully suggest that as this bill moves forward, it will be important for the people of the United States for our own national security to ensure that those sorts of authorities remain tied to the Director of the National Cyber Center.

I believe that the private sector advisory council is very important and urge that, too, be implemented. I will say, however, since leaving government, I often hear from frustrated chief executive officers (CEOs) that the U.S. Government and DHS, in particular, have at times been both unresponsive and not engaged with them. We should look at existing mechanisms before creating new advisory councils. The President has the National Security Telecommunications Advisory Council (NSTAC), and the National Infrastructure Advisory Council (NIAC), which reports to the President through DHS. These exist now and must be used, but they need interaction and dialogue with the President of the United States, not just with the White House and agency staff.

Third, as addressed in Section 251 of your bill, information sharing with the private sector must be a two-way street, and sensitive commercial data must be explicitly protected.

Last, while the bill creates both the White House position and the DHS center, both positions are Senate-confirmed. And while I understand why that is so and I strongly support congressional oversight, I believe that the position in the White House must be left to the President's prerogative to decide how to adequately staff it and, thus, do not necessarily believe that the White House position should be Senate-confirmed.

I applaud the Committee's focus on this important issue and hope that this legislation as it proceeds will only be further strengthened and not diminished by compromise. The goal is to make a positive and meaningful contribution to the national security of the United States, and this bill goes a long way towards achieving that goal.

I thank you and look forward to answering your questions.

Chairman LIEBERMAN. Thanks very much for that very helpful testimony.

I do want to say at this point that we had intended to have Robert Jamison as a witness. He is President now of the Eline Group and former Under Secretary at the Department of Homeland Security during the Bush Administration, where he was the senior official on all cyber and communications operations. Unfortunately, he was not able to attend because of a family emergency, but his testimony, I think, is quite strong, and we have left copies of it on the tables for those who are interested.[1]

Next, we are pleased to have Alan Paller, Director of Research at the SANS Institute and former member of the National Infrastructure Assurance Council, widely recognized as an expert in cyber matters. We are glad to welcome you back to the Committee and look forward to your testimony now.

TESTIMONY OF ALAN PALLER,[2] DIRECTOR OF RESEARCH, THE SANS INSTITUTE

Mr. PALLER. Thank you, Mr. Chairman, Senator Collins, and Senator Carper. You made last Thursday a very good day for the people who had despaired the government would ever lead by example. So it was just a wonderful day that you made for us, and the bill that you put together actually solves sort of the main problems that had kept the government from doing the right thing. I will summarize a few of them.

Before I do that, part of the bill is this little thing called the cyber challenge, and Senator Carper has been just wonderful at helping it. But I wanted to come back to you, Mr. Chairman, because last August you met with a young man from Connecticut named Michael Coppola who, at 16 years old, beat all these adults in a major competition. He was moved by that. While he was in school, he was asked what were the courses that the high schools are not teaching that would have allowed the other students to do well. So we outlined the courses, and I said, "That is good. Can you

[1] The prepared statement of Mr. Jamison appears in the Appendix on page 116.

[2] The prepared statement of Mr. Paller appears in the Appendix on page 84.

give us a syllabus?" He said yes and he built a syllabus. And I said, "That is good. Can you give us the exams that you would give to see if the people had learned it?" And he did that with some friends.

About that time, the State of California was getting ready for the California cyber camp. I heard your song on Thursday about the cyber camp. But they wanted to go to the high schools, and we went to the high schools, and none of the high school kids had ever seen cyber security. They did not know what to do with it. So they could not take the exam that the college kids were taking that was a real cyber security exam. So we took Mr. Coppala's exams, built a competition; 150 high school kids took it. They took hours and hours and hours out during the weeks they had AP exams, I mean, they were so excited about it. Governor Arnold Schwarzenegger personally came to give them—or he actually wrote the letters that recognized the winners of it. It was a very nice thing. So your 16-year-old from the high school that does not even have a programming course did awfully well.

Chairman LIEBERMAN. That is great to hear. Thank you. I am proud of him. And he won a contest, as I recall.

Mr. PALLER. Yes, he beat a bunch of adults and other people in a King of the Hill cyber competition, a tough one.

Chairman LIEBERMAN. I am glad he is on our side.

Mr. PALLER. Exactly right.

The most important parts of your bill are the ones that reduce our vulnerabilities because we have so much of our existence dependent on the Internet, we are much more vulnerable to an attack. Even if an attacker has lesser capabilities than we do, they could do much more damage to us because we are so dependent on it. We can take out other people's capabilities, but they are not hurt as much. So our ability to defend ourselves completely is actually the only first—and you do first things first. It is the only thing we have to do first. And what you did in the bill is you enabled that, and I want to tell you why—because I think there will be pushback, I would sort of like to give you why I think it worked.

The White House office was controversial the last time, and I was so happy you went ahead and put it in the White House. And the reason has nothing to do with whether DHS can or if the White House is better. It has to do with this cross-agency action that nothing any one agency does ever moves another agency. It is not until somebody in the White House beats them about the head and face that they actually move. And so putting it back in the White House under a tough boss can actually make a difference. And you gave it the right authorities to do that.

The reason is that we have this odd attitude about security where we get mad at people for not defending themselves well. So we talk about the government is not doing a good job of defending themselves. It is the wrong order.

Remember, we train tens of thousands of people a year to defend things, so we know what they can and cannot do. You cannot defend yourself using the off-the-shelf tools that the vendors sell you. You cannot defend yourself using the networks that the internet service providers (ISPs) provide to you. You cannot. You can barely survive at that level.

The only way to actually do the defense is a partnership between the users—think of them as automobile drivers—and the car manufacturers, the people who sell the IT services and software and the people who sell the IT online services, the ISPs. It is a partnership. They have to get better and the users have to get better. But it is cheaper for the vendors to say you users are bad drivers. We do not want to fix our cars because you guys do not drive well. It is the partnership. When the cars got safer and the people drove better, we actually had a lot fewer accidents on the road. That is what we have to do. But you cannot do that without procurement because none of those vendors will listen to any user except a very large user. So you need cross-agency buying, and the only way you are going to get cross-agency buying is with that White House office.

So I am trying to put the pieces together. You cannot have procurement without that White House office because no one else has the power to pull the money together to make it spend together.

The third one is the regulatory framework you put in. If we do not get that right, we have no defense on the civilian side—no recovery on the civilian side. I read this article about unintended consequences. The industry is saying there may be unintended consequences, and I had this immediate image of all the taxi drivers setting up a block so that the military could not get in to stop traffic because the taxi drivers needed to keep on making their money with tolls. And there is a nuclear bomb that the army was trying to stop, and the taxi drivers said, "Look, there are unintended consequences of you coming. Could we have a meeting? Can we talk about it?" I had this exact image of them. It might not be fair to share. But somebody is making money, and they really do not want to stop for anything. I guess that is all right.

But I do want to go back to this procurement thing. There are actually two sides. We have this idea that we need to protect our systems. We keep talking about that. We will be able to do that well if we do all the things that you are talking about, and I am going to show you a cool thing that one of the agencies has done—that Senator Carper found, actually—that will actually make a huge difference in that. But once we get the hygiene right—that is Bob Dix's old word. Once we get hygiene right, people will still make it through. There are organizations with enough money that they will, in fact, get through all the defenses when we have as perfect defenses as we can. So there is another half—and it is literally a half—which are the people who the air force has given a wonderful name to—they are called the hunters, and they are the people who can unravel the data about an attack, figure out what it is and what they are doing and how they are doing it and stop them. So you helped set that up. The reason that DHS is having such trouble relative to DOD is they have none of those hunters. And all these people they are hiring are not hunters because you need seeds for the crystal, and they do not have any seeds there. The seeds are all at NSA, and when they are hiring 300 more people, when you go look at their skills, they are just not the hunters. They are not the people we have to have.

In closing, I want to tell you about a wonderful positive story. There is a concept of reducing risk. This is a chart that shows every embassy around the world and every State Department office around the world over 12 months, a reliable measurement of cyber security risk, reliable as in the NSA has been there to say, yes, they are doing pretty good. And it is a 90-percent reduction in cyber risk in all of the embassies and 89 percent across all the State Department offices. This ended in August just this year. They are almost half again as good. This is the model that you will not find in any other agency around government. And it is a model that actually gives us response. When the Google hack happened at all agencies—it was an Internet Explorer vulnerability. We all had Internet Explorer. So every machine had this. Every agency sent out emails saying fix it, fix it, fix it. State did not say fix it. State actually changed the risk score on the vulnerability. It is called the Aurora Vulnerability. They changed it. So when you talk to DOD, they will tell you, "We got 70 percent compliance in about 4 months." If you talk to other agencies, 60 percent, 50 percent. State Department got 90 percent in 6 days. So 4 months, 70, 60 percent versus 90 percent in 6 days. This is what continuous monitoring is all about.

Maybe one last thing, or am I way over my time?

Chairman LIEBERMAN. You are way over, but one last quick thing.

Mr. PALLER. So the reason agencies could not do it is this: The last FISMA gave the power to set standards to the National Institute of Standards and Technology (NIST), and they had no adult supervision. So it wrote a standard that said that one of its guidance documents was mandatory, and that guidance document required all of these, 8,511 pages, that you have to do every day, and I am sure that all cyber security will. But, anyway, that is it.

Chairman LIEBERMAN. That was great. Thank you. You are the most mobile witness we have had before the Committee in a long time. [Laughter.]

Thanks for your excellent testimony, and I appreciate your words of support for what we have proposed here.

Next we have Steven Naumann, who is Vice President for Wholesale Market Development for Exelon Corporation and Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC). Mr. Naumann is going to be testifying today on behalf of the Edison Electric Institute (EEI), which represents about 70 percent of our electric sector, and the Electric Power Supply Association (EPSA). Thanks very much for being here.

TESTIMONY OF STEVEN T. NAUMANN,[1] VICE PRESIDENT, WHOLESALE MARKET DEVELOPMENT, EXELON CORPORATION, ON BEHALF OF THE EDISON ELECTRIC INSTITUTE AND THE ELECTRIC POWER SUPPLY ASSOCIATION

Mr. NAUMANN. Thank you, Chairman Lieberman, Ranking Member Collins, and Senator Carper.

Just quickly, Exelon serves more than 5.4 million customers in the Chicago and Philadelphia areas. We operate approximately 30,000 megawatts of generation, including 17 nuclear units, just to

[1] The prepared statement of Mr. Naumann appears in the Appendix on page 101.

give you an idea of our scope. And as you said, I am representing EEI and EPSA today. We are members of both trade organizations.

At the outset, I would like to thank you, Chairman Lieberman, Ranking Member Collins, and Senator Carper, for your thoughtful approach to the bill and for your leadership on this issue. The owners, operators, and users of the electric power grid take cyber security very seriously. In fact, a broad coalition representing the full range of generation, transmission, and distribution interests in the United States as well as regulators, Canadian interests, and large industrial customers all agree on the need for government involvement in protecting critical infrastructure from cyber attack. While I am not testifying officially on behalf of the coalition, this cooperative relationship to address threats to the power grid is vital to improving cyber security.

There are three principles in the bill that I would like to emphasize: First, leveraging public and private sector expertise, including information sharing between the two areas; second, concentrating on truly critical infrastructure; and, third, addressing cyber security in a comprehensive, multi-sector way.

First, both the government and the electric power sector have distinct areas of responsibility and expertise. With its intelligence-gathering and law enforcement capabilities, the government is able to detect threats, evaluate the likelihood of malicious attacks, and identify patterns of potential infiltration. Power companies, on the other hand, are experienced at operating their systems and engineering resiliency and recovery, depending on a threat.

To best ensure the cyber security of the Nation's electric grid, we need to clearly define these roles and responsibilities while facilitating cooperation and information sharing between government agencies and the power sector. The government-wide coordinator your bill envisions is critical to ensuring that information does not fall through the cracks and that the right people have complete information to make sound operational decisions in times of crisis. This careful consultation with industry helps ensure that government actions in protecting the grid from a cyber attack do not have unintended or harmful consequences, and I will be glad to explain that I do not mean taxi drivers blocking the streets, but when you are operating a system, if you do not do the right thing, you might get things happening that you really do not want to.

Second is the bill's narrow scope. It focuses appropriately on the need to protect truly critical assets and deal with cyber security emergencies. There is a security axiom that states, "If you try to protect everything, you protect nothing." Therefore, the risk-based prioritization reflected in the proposed bill ensures that both government and private sector resources are allocated wisely.

The industry believes your bill focuses on the more relevant question and urgent security gap. What additional authority is needed in order to promote clarity and focus in response to national cyber security emergencies?

Third is the comprehensive approach to dealing with cyber security. While the electric power industry's focus is on operating and protecting the electric grid, the interconnected nature of our critical infrastructure requires a multi-sector approach. We in the power industry rely on telecommunications systems to operate the grid, pipelines and railroads to bring fuel to our generation, and wholesale markets to sell our product. Should any of these critical sectors be compromised, the reliability of the electric power system would be impacted. Likewise, each of these sectors depends on a reliable supply of electricity to operate. Your bill recognizes this truth, as did the President's "60-Day Cyber Review" completed last year. I would urge the Congress to follow your leadership and approach this issue holistically.

Again, the industry's perspective on sound cyber policy includes promoting clearly defined roles and responsibilities, as well as ongoing consultation and sharing of information between government and the private sector. Using a risk-based model that secures truly critical assets against cyber security emergencies is the best use of the limited security resources and approaching the issue in a comprehensive, multi-sector way.

Again, I appreciate the opportunity to appear today and would be happy to answer any questions. Thank you.

Chairman LIEBERMAN. Thank you very much, Mr. Naumann.

Finally, we go to Sara Santarelli, Verizon's Chief Network Security Officer. I hope that you will be able to offer us a perspective on the type of intrusions and probes that Verizon is seeing on a regular basis, but thanks for being here.

TESTIMONY OF SARA C. SANTARELLI,[1] CHIEF NETWORK SECURITY OFFICER, VERIZON COMMUNICATIONS

Ms. SANTARELLI. Thank you for having me today. Mr. Chairman, Ranking Member Collins, and Members of the Committee, thank you for the opportunity to discuss this important topic of cyber security today.

Your legislation represents a positive step forward. We feel that the majority of the legislation supports the common goal of creating a much safer online environment, even if we may not agree with every specific provision.

Cyber security initiatives take place at many different layers at Verizon. We work closely with our suppliers to help ensure that their products meet our security requirements. We use technologies to identify and mitigate threats on our network. We have developed an internal dashboard to help manage security of our own corporate systems, and we offer a wide range of services to our customers to help them better protect their networks and their data.

Security events are a constant reminder that our networks and our customers' networks are under steady assault. These threats are constantly changing and evolving as criminals develop new techniques to get around the latest defenses, and once launched, these attacks can escalate with an astonishing speed. Speed and flexibility are critical to the success of our response.

The Slammer worm, launched in January 2003, was the fastest spreading computer worm in history. It doubled in size roughly every 8.5 seconds. Within 3 minutes, the worm had achieved its full potential with more than 55 million computers being scanned per second. Success in stopping the Slammer worm was predicated on the ability to take fast and decisive action without extraneous

[1] The prepared statement of Ms. Santarelli appears in the Appendix on page 109.

briefing, consultations, or declarations. Similarly, the experience in 2009 and 2008 as well with the Conficker worm illustrates how important it is to maintain a flexible approach in responding to cyber threats.

In response to this threat, an international working group was actually formed consisting of 30 named members and many more partners and contributors from around the world, including Verizon. Information sharing by that working group proved very effective.

Each incident we respond to teaches us different lessons, but the one common denominator is this: While government has a role to play in enhancing cyber security, it must not act in ways that diminish our flexibility, speed, and independence that network providers find essential in waging the war on cyber crime. Any government-directed information-sharing mechanism must not place restrictions or requirements on the free flow of information about the Internet and must not deter participation by knowledgeable entities.

Network providers like Verizon are on the front lines of this war, but the fight cannot be left solely to the private sector. There is a role for government to play. We applaud the Committee's efforts to help bring clarity and definition to that role.

The government can do things that the private sector simply cannot. My written statement identifies eight ways in which the government can be uniquely helpful. Let me summarize three.

First, the government should lead by example, working to enhance the security of public networks, centralizing, clarifying agency roles and responsibilities; eliminating regulatory duplication; and purchasing technology solutions that raise the level of security technology in the marketplace generally. Proposals in this bill would help streamline public-private interaction and ensure consistency in the security of the government's infrastructure. The bill also takes several positive steps towards eliminating duplication, enhancing the security of government networks, and using the government's budget power for targeted investment in cyber security technologies.

Second, the government should promote enhanced security for private sector infrastructure but not at the expense of speed and flexibility of response. For those who are slow in adopting best practices in the areas of cyber security, it is appropriate for government to provide strong incentives for them to do so. However, given the wide range of networks and technologies, as well as the rapid pace with which cyber threats are evolving, we simply cannot lock ourselves into a single regulated approach. The most effective approach, which this bill does take, is a public-private partnership where government provides assistance and expertise to the private sector. Confidentiality and liability protection will encourage the private sector to implement desired activities.

Finally, the government should eliminate legal barriers to the collection, use, and sharing of information by network operators, their customers, and the government. Striking an appropriate balance between privacy and the need for information sharing will directly support our shared goal of enhanced cyber security.

We look forward to continuing to work with you and the Committee on cyber security legislation, and I look forward to answering your questions today.

Chairman LIEBERMAN. Very good. Thank you. We will do 7-minute rounds of questions.

Ms. Townsend, since you have been liberated from official Federal service, maybe you can respond more directly to some of the questions that were asked of Mr. Reitinger, which are, really, who would you say are the main sources of attack against American cyber systems?

Ms. TOWNSEND. Sure. I mean, I think if you look at the open source material that is available, it is commonly understood that our most capable adversaries, potential adversaries are both the Russian government and the Chinese government.

Chairman LIEBERMAN. Right.

Ms. TOWNSEND. We have capable allies, of course, in Western Europe in the British and the French, but, of course, once you know you have capability, how they use it is really dependent on their own agenda.

Chairman LIEBERMAN. Do we think that the non-state actors, both terrorist groups and organized crime syndicates, are developing the capacity to cyber attack us or others?

Ms. TOWNSEND. It is an interesting question, Senator, because I think our understanding as you watch terrorist organizations, in particular, is that their operational capability is often dependent on their ability to use the Internet. Whether that is to pass information, propaganda, recruit, or fundraise, they need the Internet just as we need the Internet. And so that sort of mutual need has been something of a protective measure in terms of their willingness to cyber attack. That is not a guarantee. And so, of course, I think the government watches quite closely how the capability of our terrorist adversaries increases and looks for the potential that they may turn and decide it is worth using it as an attack method.

Chairman LIEBERMAN. Thanks for those answers. They are very helpful.

I appreciate very much that both Mr. Naumann and Ms. Santarelli are here because you represent major private sector entities that are affected. And I know that both the corporations that you work for and the sectors of the private economy that you are associated with are aware and sensitive to the threat in cyberspace, and that it represents a threat not just to your businesses but to our national security if a vulnerability is tapped.

So I wanted to ask you—and then Mr. Paller and Ms. Townsend if they want to get in this question: Obviously, this legislation is premised on a conclusion that there is a need for governmental involvement. We try very hard to have a balanced, collaborative public-private sector approach in the bill. But there are some who might argue that there is actually little or no need for government involvement here because industry has the same incentive that the government has to secure its networks. And I wanted to ask you if you agree with that, and if you disagree, why. In other words, is there a necessary role for government here?

Mr. NAUMANN. Chairman Lieberman, the electric power industry believes there is. As I said in my remarks, we all take protection of our networks very seriously, and for the reasons you state. But our capabilities do not go to intelligence gathering. They do not go to evaluation of some of these threats. We need to be able, first of all, to be notified of these threats. We need to be able, working with the intelligence agencies or those who have that information, to understand how those threats can affect our equipment and our service to our customers, and then to devise mitigation measures together with the government.

We simply do not have that ability, nor, obviously, is that our expertise. Our expertise is running power systems. And so as I said, there is this gap. Could it be filled in some informal way? Yes, but the problem is when you get into a real emergency, there need to be lines of communication and procedures that are set up, practiced and drilled so that we know that information will get down to the people who need to actually put it into effect.

Chairman LIEBERMAN. Ms. Santarelli.

Ms. SANTARELLI. Senator, when I look and I think about how can the government help the private sector, I think it is important to understand that the ecosystem of the Internet is actually made up of multiple layers. We have the suppliers of equipment and information systems. On top of that, that equipment and the systems are pulled together to make the infrastructure. On top of that, we have applications and systems that ride and the content that rides on the network. And then beyond that, connecting it all together, we have our end user population. I like to call it Grandma and Grandpa checking out the Internet at night or our kids that are on Facebook or whatever.

So when we look at this as from a pure network provider perspective, we are just one part of the ecosystem, and I do not think any one part has the power or the ability to drive a solution in terms of security threat. All of those layers need to work together, and I think that government can help us with that.

You note in the bill in particular the dispensation for security controls on your vendors. As one of the largest purchasers, we would like to see the government definitely drive that into our equipment providers so that as we take that equipment and build networks and applications with equipment that does have the security requirements.

Chairman LIEBERMAN. Very good. Would either of you like to add anything? Ms. Townsend.

Ms. TOWNSEND. Senator, just very quickly, of course, the government is the only entity capable of prosecution of crime, and so you are going to see acts that are crimes. But I would also note that in the intelligence and national security arena, we have seen instances in Estonia where one might rightly classify a cyber attack as an act of war. And so the government must play a role in working with the private sector. I absolutely believe the government cannot run it uniquely, and I have talked to the issue of the need for a public-private partnership. But we would be remiss if we did not believe that the government has a very substantial role.

Chairman LIEBERMAN. This is a most unusual area because we went for long periods of our history—after the initial chapters of our history—without being attacked here in our homeland, with the blessing of the protection that the oceans gave us. Then came

Pearl Harbor, then another long period when we feared attack but there really were not any any during the Cold War. Now, unfortunately, we have been regularly the target of attack by the Islamist terrorist movement. But now in a way that is really totally unprecedented, through cyberspace, we can be attacked from far away here in our homeland. And it seems to me that perhaps the most attractive, if I can use a bad adjective, targets for an enemy will be private sector targets because of the extent to which our society depends on them, whether the electric grid or a dam that is holding back an enormous amount of water that is controlled over the Internet.

I appreciate the answers that all of you gave, and to me it really cries out for the kind of public-private collaboration that we are talking about.

My time is up in this round. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Ms. Townsend, I had a discussion with the previous witness about the existing emergency authorities of the President that were passed in the wake of the attack on Pearl Harbor in World War II. Let me get your opinion on this issue. Do you believe the existing emergency authorities, the authorities in current law, are sufficient for the President to deal with cyber attacks?

Ms. TOWNSEND. Senator Collins, thank you for the opportunity to address that question. I can say unequivocally my belief is that the existing authorities are not adequate, and they are ambiguous, as you noted.

I would say in the Cyber Shockwave exercise that I had the privilege to participate in, Jamie Gorelick, the former Deputy Attorney General in the Clinton Administration, acted in the role as the Attorney General, and she said that existing authorities are not only inadequate, but that in the absence of adequate authorities, she made the point that a president in a crisis will act and look to right it later with the Congress and the American people.

I do not think that is the way we want to behave. I think you quite rightly point out that we ought to tackle the tough problems up front and make sure that the President and the Executive Branch have the authorities they need to act and that we are comfortable balancing security versus privacy and civil liberties.

Senator COLLINS. Thank you. That is excellent testimony, and your point is very well taken. A President is going to act, and that is, frankly, also where you see abuses, where there are problems when there is not clear authority. So since it is so evident that cyber attacks are happening every day and are only going to get worse, it just cries out for us to establish the rules now in a thoughtful way.

Mr. Paller, I want to bring up a different issue with you which was prompted by your demonstrating your extraordinary knowledge of what is going on in the Federal Government. If government agencies, as required by our bill, coordinate to establish a government-wide security standard or set of standards for the purchase of IT products, do you believe there would be a favorable impact on price? In other words, if that happens, is there a potential of saving taxpayers some money in these purchases?

Mr. PALLER. Thank you for asking that question. It actually not only will save money for the government, it will actually make a lot of money for the vendors. The same vendors that say, no, you are a bad human being to ask for that are going to make a lot of money. Here is the example.

Do you remember when the Department of Veterans Affairs (VA) lost 17 million pieces of information?

Senator COLLINS. Yes.

Mr. PALLER. Everyone wanted to encrypt their laptops. There were millions of laptops in the government. The commercial price for a laptop encryption was $243. The General Services Administration (GSA) price was $97. It was not enough. I mean, they did not have enough money to buy that.

They got together, the White House, DOD, the States actually got together, pooled their buying. They did not pick one, they picked several. So it was not we are going to define you are the winner, everybody else is the loser. But they picked several, and they negotiated prices in which that price went from $97 to $11 in the first buy. But the amount of money that the software—I built a software company. We in the software business want the revenue. It is not the price per package. Buying millions of copies at $11 still makes us a whole lot more money than your buying five at $100,000 apiece.

So what you do when you do the buying together is you lower the price across government, but you also radically expand their market, and they make more money. And the ones who win that actually go on to take over markets all across the world because they were the ones that were selected for the government buy. It is a win-win kind of operation.

Senator COLLINS. Thank you.

Mr. Naumann, your company operates in more than one sector of the economy, and thus, you are regulated by various Federal agencies. For example, you operate nuclear plants, correct? So you are under the Nuclear Regulatory Commission. You also operate an electric transmission business that is regulated by the Federal Energy Regulatory Commission (FERC). So because you have experience in dealing with different regulatory agencies, I want to get your view on the need to have a Federal agency involved in addressing cyber security in a coordinated way across all the critical infrastructures.

In other words, if we do not act to make clear who is doing what in cyber security, are you likely to be subject to different standards by different agencies?

Mr. NAUMANN. Thank you, Senator Collins. That is correct. At present, I will tell you the agencies, for example, the NRC and the FERC through the North American Electric Reliability Corporation, are trying to coordinate their cyber security policies. Of course, that does not include, for example, in our case the Illinois Commerce Commission, which has authority over our distribution network, and the Pennsylvania Public Utility Commission, which has authority over the network in Pennsylvania.

Having one set of best practices, including the feedback that the legislation contemplates of being able to go back and showing how we would solve a problem, I think would make it easier not only for us; it would make it easier for the various regulatory organizations and be more cost-effective. So we would support a single agency being the coordinator and then cascading down.

Senator COLLINS. Ms. Santarelli, same question for you.

Ms. SANTARELLI. Yes, Senator Collins. Thank you for the opportunity to comment on that. As a national infrastructure provider, we agree with Mr. Naumann that it would be beneficial to us to have a single one voice into the government entities rather than having to work through multiple entities. As I mentioned in my oral testimony and my written testimony, it is very important to us to continue to have the speed to respond to any threat in near real time, if not real time, and working across multiple agencies I think could complicate that ability.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Senator Carper.

Senator CARPER. Thank you, Mr. Chairman. I just want to observe, if I could, to our Chairman and Ranking Member that the subject that is before us today can be pretty dense and pretty hard to understand. And I say that as a guy who, until just a couple years ago, could barely spell the word FISMA, and today I actually understand what it means. And you have taken some tough, complex subjects and made them really understandable, even for me, and I thank you for that. Really good presentations and answers.

I have heard from Mr. Paller a number of times before, and I have always observed that your presentations are, I think, especially effective. Have you ever thought of writing a book on this subject?

Mr. PALLER. If you look at my written testimony, it is really long. [Laughter.]

Senator COLLINS. He already has.

Senator CARPER. Fair enough. Sometimes I start off my questioning when we have a second panel, I ask the second panel to look back at the testimony of the first panel and ask if there was anything that you especially agreed with or disagreed with from our first witness. And then I just want to ask you to kind of play off of each other and ask you to think about some of the things that your colleagues said during their testimony, and say, “Well, I really agreed with that,” or, “Boy, they are out to lunch on that one.” But go back to the first panel with us. Anything that was said that you especially want to underline or emphasize for us. If you would just start off, Ms. Townsend, please.

Ms. TOWNSEND. Thank you, Senator. I do think I was struck by Senator McCain’s question about partnership and Phil Reitinger’s answer. A quick vignette, I led the Katrina lessons learned about how we could do things better, and I remember interviewing General Russ Honoré, and we talked about the national incident commander’s role to coordinate the response. And he had this great line that I never forgot. He said, “You know, when you have a coordinator, a coordinator starts out to make a horse and ends up with a camel.” And it was graphic enough and there is something to that.

And so I do think we have to be careful. That is why I said if DHS is simply in the role of coordinating, somebody does need to lead. Senator McCain is quite right. I think DHS is right to lead, to understand where greater capability in the government may reside to protect defense systems, intelligence systems, but somebody must lead. I think that makes it especially important that you have a White House office. Everybody needs a Daddy, and if this is——

Senator CARPER. And a Mommy.

Ms. TOWNSEND [continuing]. Inside DHS, that person will need the gravitas of a White House office to break through the interagency process that can only be done there. And so I do think we have to be careful to make sure to give them the authority to actually get the job done and then the link to the White House to implement it.

Senator CARPER. All right. Mr. Paller.

Mr. PALLER. Only one. When Mr. Reitinger was talking about the people and how critical the people are, I think he was radically understating the problem. A man named Jim Gosler, who ran the Clandestine Information Technology Office (CITO), in the Central Intelligence Agency (CIA), said to a bunch of people in the Pentagon and NSA, "We have only a thousand people that can fight at world-class levels right now." There was another person at the meeting who was a senior DOD official that was frowning, and I asked him why he was frowning, he said, "Because I cannot get to a thousand." We need 20,000 to 30,000 of those people.

The problem with what Mr. Reitinger is doing, is he is trying to hire them away from other people. But if you only have a thousand, you are just going to grab them from a DOD contractor or a NSA contractor. He has to change his mood from we are going to go get these people to we are going to go build these people, and he has to really take that on. His legacy is the building of those people because until DHS has that core of excellent people who are not contractors but are inside the organization, they cannot compete with NSA and they cannot defend the Nation.

Senator CARPER. Good point. Thank you. Mr. Naumann.

Mr. NAUMANN. Senator, actually it was something you said about——

Senator CARPER. Something I said?

Mr. NAUMANN. Yes, sir. The difference between what is on paper and implementation. And for the electric power industry, when there is an immediate threat, having a single point of contact to cascade that down with communications protocols and channels that have been drilled and practiced is essential. When time is of the essence, there is no time for confusion. And so having the clear chain of command to get the information to us, to be able to work with us to devise mitigation, and get that information out to the right people becomes essential. And that involves the implementation and it involves drilling and it involves getting it right.

Senator CARPER. Thank you. Ms. Santarelli.

Ms. SANTARELLI. Thank you, Senator Carper. When I was listening to Mr. Reitinger's testimony and he spoke of a recent worm, Conficker, he shared some of the difficulties in working through all of the different agencies and getting information, it struck me because in my oral comments I referenced the same worm. And in the private sector, it was a different experience. We very quickly pulled together a working group that stands over 30 entities strong with a lot of additional partners outside of that, a worldwide group of folks, technical folks coming together to share, “Hey, what worked for you? What is the issue? What are you seeing?” “Hey, here is this IP address. Here are where the machines are that you need to avoid and not interact with them.”

And so it struck me that partnership is important and that we should learn from each other, because on the one side it works so well in the private industry to be able to share that information live, and we would really look forward to working with the Committee to share some of those best practices that we have in our ability to communicate and interact with organizations like SANS and others to share that information. Thank you.

Senator CARPER. Thank you. One last quick question, if I could. My colleagues have heard me say from time to time that the role of government is to steer the boat, not row the boat. And another thing that has fascinated me for a long time is how do we use market forces to try to drive good public policy behavior?

Let me just ask, for those two principles, for me cardinal principles, how well do we do in terms of measuring up to those principles in the legislation that we have introduced? Ms. Santarelli, do you want to go first?

Ms. SANTARELLI. Yes. I think that there are some really positive aspects in the legislation that you have introduced. I do like the ability to continue to grow in terms of the public-private partnership. I think that there is improvement in opportunities where we can work together to share information.

I would like to see and continue to work with the Committee to address some of the legal barriers that we believe are there that restrict us a bit in terms of being able to share information. So we would like to see those barriers ironed out a bit to ensure more success in our ability to share information.

Senator CARPER. Thanks. Mr. Naumann.

Mr. NAUMANN. What this bill does is it puts an overlay on the security and reliability processes the industry has now through the North American Electric Reliability Corporation setting mandatory standards. It acts or puts into place something that really the government is the one who has that capability on the intelligence gathering.

There are processes now. What is contemplated here is better because, as I said earlier, you need certainty and also the feedback in providing industry solutions back to the government to get the best solutions. And so what it does is it lets us do what we do best, and we do set through NERC cyber security standards. But it puts an overlay on that for the part where the government has the real expertise, and that is simply not our—intelligence gathering is not our job.

Senator CARPER. All right. Mr. Chairman, could we hear just briefly from Mr. Paller and Ms. Townsend?

Mr. PALLER. I give you a 9.1. It is really well down.

Senator CARPER. Was that on a scale of 100?

Mr. PALLER. On a scale of 10—9.1.

Senator CARPER. Thanks. Ms. Townsend, last word.

Ms. TOWNSEND. Yes, I think the liability protection provided in the bill is incredibly important for the private sector. If there is something I would strengthen, we have to protect the information that we are encouraging be shared, and I think that is important whether it is traveling from the State and local level all the way up through the Federal Government to the private sector or the other way. We have to ensure that across the spectrum of shared information we are making sure that the information is protected, or the private sector will not share.

Senator CARPER. All right. Thank you all very much.

Chairman LIEBERMAN. Thank you, Senator Carper.

Senator CARPER. And, Mr. Chairman, thank you very much for allowing me to a be a part of this trio, and I think we are on to something good here, and we very much look forward to working with you.

Chairman LIEBERMAN. Thank you. Our pleasure to work with you, and you did say something, just in answer to your question.

I want to just highlight—and then we will let everybody go—this last exchange because there is something I came to appreciate as we worked on this bill, and Senator Collins particularly made a very significant contribution on this point, which was that when we talk about the emergency authorities of the President with regard to the most critical parts of cyberspace, a lot of what we are talking about is the importance that the President has the capacity to say to an electric company or to say to Verizon in the national interest, "There is an attack about to come," or "We are in the midst of an attack, and I hereby order you to put a patch on this or put your network down in this part or stop accepting anything incoming from Country A."

That might be the kind of thing that an individual company would want to do or know they should do, but the potential liability in doing that is enormous, because in the normal business sense, you might well be putting down operations with enormous financial consequences or losses. But it is in the national interest to do that at that moment to stop greater losses.

So I wanted to explain that just in this last line of questioning and your answers to Senator Carper because that is really what we have in mind. There is no authority here, as Senator Collins said at the beginning, for the President to have the government take over cyberspace. It is really through the National Cyberspace and Communications Center at DHS to issue orders probably as a result of previous agreement and collaboration with the private sector, to do things that in a normal business sense you would be hesitant to do, but in terms of national security there is no question that you should do it, and we should protect you from liability.

Do you want to add anything to that, Senator Collins? You made a very important contribution to that part of the bill.

Senator COLLINS. Thank you. Mr. Chairman, I do think that we got that right, and I very much appreciate the strong testimony in support of it.

I just wanted to make a couple of final comments. This is very complex legislation dealing with an extraordinarily important issue, and I want to thank our staffs and all the private sector partners that assisted us in drafting this bill. I think that is why I will say that I believe we have come up with the best approach of all the bills that are out there. It is because we did get a great deal of advice, insight, and input from the private sector partners, from former government officials, and from current government officials.

So I just wanted to thank those individuals, many of whom are here or are represented here today, as well as our staffs for their hard work. This has been a long time coming, but I think we have produced a very good bill, and I thank you for your leadership as well.

Chairman LIEBERMAN. Thanks, Senator Collins. You are absolutely right. It took longer than we wanted, really. A lot of it was because there was a lot of consultation. We tried to do this in a collaborative way, and as a result I think it is a better bill.

Incidentally, we took a long time in getting to this point, but now we have our foot on the gas, because this is really urgent. So we are going to report the bill out hopefully next week, and as I said earlier, I believe Senator Reid is going to try to bring the various bills together to reconcile differences and then schedule floor time this year to move this along.

This has been an excellent panel. You have been helpful to us before today and today. I thank you very much for that.

We will leave the record of the hearing open for 15 days for additional statements and questions, and with that, I thank you and adjourn the hearing.

[Whereupon, at 5:08 p.m., the Committee was adjourned.]

SECURING CRITICAL INFRASTRUCTURE IN THE AGE OF STUXNET

WEDNESDAY, NOVEMBER 17, 2010

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

The Committee met, pursuant to notice, at 10:07 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Coons, and Collins.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. I apologize for being a little late. I was set to introduce a nominee for a State Department position at the Foreign Relations Committee, and they started a 9:30 hearing at 10 o'clock, so I will blame it on them. But they blamed it on Secretary Clinton, so the line of accountability continues.

In a sense, this is a hearing to both remind us and educate those who are watching—hopefully, the public and Members of the Committee—about the reality of the cyber threat to the United States and how important it was that we work hard to develop cyber security reform legislation in this Congress, and how unfortunate it is that the clock is going to run out on us before we have a chance to complete negotiations with other committees and with the Administration, who I regret to say, I think did not engage as early and as fully in the process of developing this legislation as was necessary.

But this Stuxnet story really takes the reality of the threat to a new level, I believe, and I think should awaken any skeptics. And there are some, of course, who think that we are overstating the threat and, therefore, overreacting in the public resources that we are devoting to the protection of our cyber systems here in America. Of course, I totally disagree with that argument.

We have an extraordinary group of witnesses here today who will not only explain to us what Stuxnet is but will, I hope, talk more generally about the cyber threat to our country.

I will say, in terms of our legislation, that it is certainly my intention—and I know it is Senator Collins'—to come back to this legislation really early in the next session of Congress and try to get it out as soon as possible. And, again, I want to say this will require more immediate and intense engagement by the Administration and by some of the other committees that claim jurisdiction here. We, of course, think we are the ultimate source of jurisdiction for cyber security matters that are non-defense, which is the Armed Services Committee. But this will be a real priority for the Committee when the session begins next year.

Because I am late, I am going to put the rest of my statement in the record[1] and call on Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. I know that we have votes starting at 11 o'clock this morning, so I am going to follow your lead. Let me just make a couple of comments.

Much attention has been paid to cyber crimes, such as identity theft, and to cyber attacks that are intended to steal proprietary information or government secrets. But lurking beyond those serious threats are potentially devastating attacks that could disrupt, damage, or even destroy our critical infrastructure, such as the electric power grid, oil and gas pipelines, dams, or communication networks. These cyber threats could cause catastrophic damage in the physical world, and this threat is not theoretical. It is real and present, and the newest weapon in the cyber toolkit that was introduced to the world in June when cyber security experts detected the cyber worm called "Stuxnet," which demonstrates to us the extraordinary capacity that a worm could have to disrupt absolutely critical infrastructure.

It is evident that the development of this very sophisticated malware was likely the work of a well-financed team of experts with extensive knowledge of the targeted systems. It is my understanding that more than 100,000 computers were infected and that the damage could have been catastrophic.

Like Senator Lieberman, I believe that this problem is urgent. We have introduced bipartisan, comprehensive legislation to deal with this threat. I personally think it is an ideal issue for the lame duck session of Congress to take up. My fear is that we will wait until we have a successful cyber September 11, 2001, before acting, so I would like to see us be proactive on this issue, and I believe our bill points the way.

In the meantime, I look forward to hearing the testimony of all the extraordinary experts that we have today to shine a spotlight on what the impact would be of an attack on critical infrastructure, an attack that this worm has made evident could happen at any time.

Thank you, Mr. Chairman, and I would ask that my full statement be put in the record.[2]

Chairman LIEBERMAN. Without objection. Thanks, Senator Collins. Just listening to you reminded me of something I heard a businessman say a couple of days ago, which is that one of the problems with our government is that too often metaphorically it waits until there are four or five major car accidents at a cross-section before it decides to put up a stoplight. And we want to make sure that we put the stoplight and the protections up before we have not just an accident but suffer a major attack.

[1] The prepared statement of Senator Lieberman appears in the Appendix on page 124.

[2] The prepared statement of Senator Collins appears in the Appendix on page 127.

When my staff presented the memo to me about this hearing, including the description of the witnesses, my reaction was we could not have a better group of witnesses. And I really appreciate both your work in this area and your presence here today.

We are going to begin with Sean P. McGurk, Acting Director, National Cybersecurity and Communications Integration Center at the U.S. Department of Homeland Security. Good morning, Mr. McGurk.

TESTIMONY OF SEAN MCGURK,[1] ACTING DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MCGURK. Good morning, Chairman Lieberman and Ranking Member Collins. My name is Sean McGurk. I am the Acting Director for the National Cybersecurity and Communications Integration Center, and up until recently I was the Director for the Control Systems Security Program and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) also at the Department of Homeland Security (DHS). The Department greatly appreciates this Committee's support in our ongoing efforts to identify cyber threats and to combat cyber concerns in the critical infrastructure, and in addition, I appreciate the opportunity to appear before you today to provide some insight into the activities that we have analyzed and identified in relation to Stuxnet.

I would like to discuss the importance of securing these control systems and how they significantly differ from the information technology systems that we have been focusing on over the past few years, and to also discuss DHS' approach in addressing cyber threats and cyber risks as they apply to the control system. And, finally, I would like to spend a few minutes discussing Stuxnet itself and how Stuxnet has changed the landscape when it comes to critical infrastructure.

Something as simple and innocuous as this becomes a challenge for all of us to maintain accountability and control of our critical infrastructure systems. This actually contains the Stuxnet virus.

Chairman LIEBERMAN. Mr. McGurk, take just a moment and define a control system.

Mr. MCGURK. Yes, sir. A control system in our common terminology is any of the automated or embedded systems that we use in our day-to-day activities. The National Infrastructure Protection Plan has identified 18 critical infrastructures in the United States. As you are all well aware, the foundational element between those 18 critical infrastructures are control systems. Energy is different than water which is different than nuclear, but the fundamental foundation is those control systems, those automated, digital-to-analog robotic systems that manufacture cars, purify water, generate electricity, or actually produce the goods and services that we rely on on a day-to-day basis.

So recognizing the unique nature of those systems, the Department created the Control System Security Program back in 2004 to address those challenges.

[1] The prepared statement of Mr. McGurk appears in the Appendix on page 129.

Much of what we have learned from information technology practices are basic principles that we can apply, but just the nature of these operational systems requires us to take a different approach in protecting them. How we protect the systems that generate power, purify our control over traffic flow systems, or our rail and aviation transportation systems is fundamentally different than the way we protect our information technology infrastructure. That is why the Department takes this all-hazards, all-risk approach when identifying those challenges.

In order to focus on that foundation, the Control System Security Program has established many activities in order to increase the level of awareness for the control systems community. One of those activities involves a Workforce Development Program. In partnership with the Idaho National Lab, we have built a very comprehensive and extensive hands-on training environment where, working with the private sector and with other Federal departments and agencies, we have been able to train over 16,000 individuals, both asset owners, operators, and vendors and other Federal agencies, in control systems security—again, focusing on the unique nature between information technology and control systems.

We have also worked closely with the standards community to ensure that we are focusing on how to apply those principles and practices from information technology into a control systems environment. It is very important to recognize those unique requirements and the differences between the systems and not try to apply a one-size-fits-all.

In order to support the asset owner and operator community in the private sector, we developed a series of tools that could be used in order to enable a self-assessment of the control systems security. There are many automated systems that enable the evaluation of information technology and enterprise networks, but we needed to focus on those unique characteristics of control systems. Subsequently, we worked with the Department of Energy laboratory community and developed these tools so that we could actually apply them in the general public.

In addition to the 16,000 personnel that we have trained, we have also trained partners in 30 different countries to increase the level of awareness of industrial control security. We actually chair an international body focusing on increasing the level of awareness for industrial control, and we have also conducted more than 50 onsite assessments at facilities throughout the United States, in 15 different States and three territories. We plan on increasing that level of activity in the coming years.

ICS-CERT also maintains fly-away teams. These fly-away teams are incident response teams that work with the private sector asset owners and operators upon request to do either remote maintenance and analysis or physical analysis. When requested, we will deploy a team. They will assist asset owners and operators in identifying restoration methods, digital media capture methods, and then we will conduct the analysis to determine what the extent of the vulnerability is and what the potential impacts are. We do this in order to understand the overall risk profile to an industrial control environment, looking at the threats, the vulnerabilities, and then potentially the consequences. And then we work closely with the community, the asset owners, operators, and the private sector to build those mitigation strategies.

When the Department first identified a vulnerability back in 2007 that we termed "Aurora"—which had to do with hacking into and modifying settings in digital protective networks, physically destroying electric generation capacity—we recognized the need to partner closely with industry so that we could develop mitigation strategies that were sector-specific. Fundamentally, what fixes the energy sector may not work in the water sector, so that is why it is important for the Department to continue to partner with those 18 sectors to identify proper mitigation strategies. We understand we need to work with the broad community in order to be effective in mitigating the risk.

We also generated fly-away team checklists. Up until this point, the understanding of what data was necessary to identify risks to control systems was not well understood, so we worked with academia and with other researchers to identify those digital capture methods so that we could actually build a forensic path to enable us to actually identify variants of vulnerability such as Stuxnet.

The Department operates a malware lab; this is a physical laboratory where we can actually install equipment and analyze how it operates. In the case of Stuxnet, we were able to configure the actual manufacturer's equipment in a live environment and not only dissect the code to determine what it is capable of doing, but actually analyze what it does once it gains access to the equipment. So that gives us a better understanding of not just the analytics behind the code itself, but also its impact in a physical infrastructure. So the Department still maintains that capability, and we share that with the general public.

We also look at our responsibility to continue to partner with the Federal departments and agencies to ensure that we are sharing the information as we analyze it. It is important for us to recognize that the intelligence community and the law enforcement community have their responsibilities in these areas, and we provide the intellectual capability behind it from a very unique skill set of industrial control to forward their efforts as well. So as we analyze the data, we share that information with the intelligence community, the law enforcement community, and other departments and agencies at the State and local level so that they understand the impacts of something like Stuxnet.

As I said, Stuxnet is a one-of-a-kind type of situation. We have not seen this coordinated effort of information technology vulnerabilities, industrial control exploitations, completely wrapped up in one unique package. For us, to use a very overused term, it is a game changer. Stuxnet actually modifies not only the physical settings of an information technology system, but it also modifies the physical settings of a process control environment.

Essentially, if I wanted to find out what the process is doing, I have the capability of removing those files or exfiltrating the data, so I do not have to break into the front door and actually steal the formula or the intellectual property of what you are manufacturing. I can actually go to the devices themselves, read the settings, and reverse engineer the formula for whatever the process is that is being manufactured. In addition, I can make modifications to the physical environment so that you would be unaware of those changes being made, and subsequently it would have an adverse impact on the environment.

So the products that you are producing may not be of the specifications that you originally analyzed because Stuxnet demonstrates the capability of bypassing the safety and security systems to go down to the root level to make those changes; so the operator may believe the indicators on the panel are accurate, but, in fact, there is malicious activity occurring at the base level. These are capabilities that we have seen demonstrated in Stuxnet that we have never seen before in any analysis of code that we have conducted.

Now, as I mentioned, there is a significant amount of concern also. Stuxnet is a pathway that people can then exploit. It has basically been a road map, and it was written in a modular format so that people could actually remove the vendor-specific payload, that malicious code that attacked the control system, and substitute it with any other type of control system code that they desire. So it was written in such a way that it allows that flexibility and capability, and that really causes us concern as we move forward. And that is why we continue to partner with the departments and agencies and the private sector to analyze the capabilities and the risks associated with Stuxnet.

Again, Chairman Lieberman, Ranking Member Collins, I appreciate this opportunity today to appear before you, and I am standing by and happy to answer any questions. Thank you.

Chairman LIEBERMAN. Thanks, Mr. McGurk. That was a very good beginning, both very informative and, frankly, chilling in terms of the effectiveness of Stuxnet. You could make a lot of comparisons to guided missiles and multiple independently targetable reentry vehicle (MIRVs) and all the rest, and from an earlier time of combat but quite something.

Michael Assante, who has a long background in this area, is currently president and chief executive officer of the National Board of Information Security Examiners. Thanks for being here.

TESTIMONY OF MICHAEL J. ASSANTE,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS OF THE UNITED STATES, INC.

Mr. ASSANTE. Thank you. Good morning, Chairman Lieberman and Senator Collins. I am coming here today in the capacity of the National Board of Information Security Examiners of the United States, Inc. (NBISE), but also a lot of work that I have done in the field of critical infrastructure protection with a focus on control system security. I am pleased that this hearing is taking place today to explore the implications of very advanced cyber threats on our Nation and our critical infrastructure. The Stuxnet code is a very worthy centerpiece for this discussion today. Even though it is, I believe, neither the first nor will it be the last attempt to compromise and use an operational system to effect physical outcomes, Stuxnet is, at the very least, an important wake-up call for

[1] The prepared statement of Mr. Assante appears in the Appendix on page 142.

digitally reliant nations; and at worst, it is a blueprint for future attackers.

My remarks today will paint a very difficult challenge, but it is important to note that I remain an optimist. This Nation, as it has done countless times in past contests, should turn to its men and women, both in and out of uniform, to muster an effective defense. Our obligation is to best organize, train, and equip these individuals to be successful in this very important task.

Stuxnet is a highly disruptive innovation. Simply put, Pandora's box was opened years ago as the United States became reliant on digital technology to help operators complete and control complex processes. Stuxnet is an important harbinger of things that I believe may come if we do not use this opportunity to learn about the risks to our infrastructures. No one should be shocked by the cyber exploits that can be engineered to successfully compromise and impact control systems. Study after study has identified common vulnerabilities found across control system products and implementations.

Stuxnet is the best example of a cyber threat that was thought to be hypothetically possible; that is, some would say the fantastic story line of those that are just spreading fear, uncertainty, and doubt. Well, in this all too real story, possible did not merely just become probable, but it snuck onto the world stage, undetected by defenders for months. Its features, capabilities, the targeted technology, and the purpose should shock security professionals, engineers, business leaders, and government leaders into action. And I say this very important statement for the following three reasons.

First, it is important that we understand there is a very well resourced group possessing the necessary motivation, who have successfully acquired the knowledge, skills, and capabilities to systematically develop and launch a highly sophisticated attack against control system technology. The now public occurrence of such a cyber attack is very important because it dispels conventional thinking that it is just "too hard" for an attacker to assemble the necessary information, gain familiarity with the technology, and acquire the knowledge of specific implementations to devise an attack that could disrupt or damage the physical components of an industrial process. It is simply not true.

What is shocking to control system security experts is not that it was done, but that it was done in such a manner as to rely upon pre-programmed code, one that had the ability to autonomously analyze the system that has been compromised and identify very specific conditions desired for the delivery of its "digital warhead."

The lesson that we must not gloss over is that highly resourced actors can assemble people and the capability to plan and to deal with system variances, anticipated security controls, obscure and proprietary technology, and complex industrial processes.

Second, we must understand that the attacks that we should be most concerned with are not designed to disable their digital targets, but to manipulate them in a very unintended fashion. Many professionals have limited their thinking to dealing with the loss of individual elements or components of their control systems and have failed to fully embrace the implications of calculated misuse.

In modern control systems, most of the process safety depends on logic that is found in the controllers. By analyzing this code, one can not only determine what the engineer wants to happen but also what the engineer wants to avoid.

Finally, our current defense and protection models are not sufficient against highly structured and resourced cyber adversaries capable of employing new and high-consequence attacks. Our defensive thinking has been shaped by the more frequent and more survivable threats of the past. This means that while current cyber defense tactics, security architectures, and tools are necessary and can be responsive to the most likely of threats, they are not sufficient to deal with emerging advanced threats. The optimist always points to a new type of security tool or practice as the solution to current protection inadequacies. But should we not believe that if it had been necessary to assure their success, the authors of the Stuxnet worm would have simply developed a way to counter any near measures that we would have fielded in force.

This requires us to consider not only security but also how we can design and engineer survivability into our complex systems and achieve a level of resilience not only in our organizations but to our technology and our processes, and better prepared to respond and recover to these types of advanced threats. The susceptibility of our modern interconnected and digitally reliant infrastructures is well established.

I would also like to spend a minute on the flaws of our current efforts to regulate cyber security. The National American Electric Reliability Corporation (NERC)-developed critical infrastructure protection (CIP) reliability standards represent a very early attempt to manage cyber security risks through mandatory standards with very significant penalties for noncompliance. It is clear to me that the standards as written and implemented are not materially contributing to the management of risk posed by very advanced cyber threats, such as the Stuxnet worm.

The standards are comprised of 43 specific requirements designed to provide what I would call a minimum set of practices that, if properly implemented, should serve as a simple foundation to built from. Many of the requirements should have already been commonplace in the industry but were not.

The standards also include significant gaps and exclusions, but their greatest weakness is in how they have been implemented. The result has been a conscious and inevitable retreat to a compliance- or checklist-focused approach to security. Unfortunately, the NERC CIP standards have become a glass ceiling for many utility security programs, which prevents the emergence of the very type of security programs we need to deal with Stuxnet-like attacks.

Regulation, although necessary, should be re-evaluated and designed to emphasize learning, enable the development of greater technical capabilities, require qualified staffs, and discourage the creation of a very predictable and static defense.

We must recognize that we are in the time of Stuxnet, and in turn, it is the time to be honest. We do not have immediate technical answers to better protect industrial control systems from Stuxnet-like attacks. We do not have an effective defenses, and we do not have adequate detection techniques. We lack a functioning information-sharing and learning framework and have limited abilities to apply new-found knowledge. The public-private partnership has failed to produce satisfactory results in these areas.

We must develop and implement protection strategies that accept the unfortunate reality that many of our networks are already contested territory. Accepting this very important assumption will help stimulate industry and community efforts to develop new and improved approaches to addressing the most material of risks.

Why did some not see this coming? Well, significant cause for concern is that much of the information about cyber security-related threats remains classified in the homeland security, defense, and intelligence communities, with restricted opportunities to share information with the cyber security researchers, technology providers, and possibly affected private asset owners.

I would like to specifically emphasize one of the necessary investments to combat advanced cyber threats like Stuxnet. Through the years, working as the chief security officer at a major utility, or by supporting researchers in a national laboratory, and coordinating protection efforts while I was at NERC, I have gained an appreciation for the importance and the difference made by skilled and well-developed people. As in this case, you must have a human complement up to the task of optimally detecting and calling out the faint signals by which these attacks sometimes announce themselves.

I have never understood why we have not embraced better training and development methods for our front-line security and operations staff. We train pilots using advanced simulators to deal with very difficult conditions and mechanical failures. Why do we not use simulators to allow security and operational staff to experience low-frequently but high-consequence attacks against systems and designs? Mr. McGurk's program that helps develop that is a great first step.

Why do we not use performance-based examinations to qualify our professionals? We have allowed chance to be our schoolhouse where targeted organizations simply suffer in silence, not willing to pass along the tough lessons that they have learned to others.

I commend this Committee for its exploration of the implications that advanced threats like Stuxnet pose to our critical infrastructure and to our Nation. We must waste no more time debating our susceptibility. We must accept that well-resourced adversaries are capable of causing damage to industrial processes in very difficult to anticipate ways. I believe the following steps are necessary.

We must remove and remediate architectural weaknesses, known vulnerabilities, and poor security designs in industrial control system technology over time.

We need to promote greater progress designing and integrating security and forensic tools into control system environments.

We must prioritize our efforts by jointly studying the potential consequences that may result from directed and well-resourced attacks of control systems and protection systems in high-risk segments of our critical infrastructure. In the cases where the consequences are absolutely unacceptable, we must assume that an attacker can successfully defeat our security and, therefore, direct our efforts to engineering away the risk that more survivable designs and practices might be able to obtain.

We need to organize a well-funded, multi-year research program to design toward a more resilient infrastructure, especially in the area of industrial and digital control systems.

We must establish new regulation in the form of performance requirements that value learning, promote innovation, and better equip and prepare control system environments and the teams that protect, operate, and maintain them. The current regulatory structure will not, in my view, be capable of achieving this end.

We must require critical infrastructure asset owners and control system vendors to report industrial control system-specific security incidents.

We must task appropriate U.S. Government agencies to provide up-to-date information to asset owners and operators on observed adversary tactics and techniques, especially when investigations reveal attacker capabilities to side-step or exploit the very security technologies we rely upon.

We must invest in the workforce that defends and operates our infrastructure systems. We need scalable, immersive, hands-on training environments, and local simulator training technology should be used to optimize the development of this workforce. The same workforce should then be qualified through periodic rigorous performance-based assessments and, where appropriate, examinations.

In conclusion, my greatest fear is that we are running out of time to learn these important lessons. Ultimately, we know that our conventional approach to more common security threats will be necessary but woefully insufficient to protect us from threats like the Stuxnet worm. We must act now to develop our greatest resources in this important contest. That would be the professionals that defend, operate, and protect the critical infrastructure and critical systems of this country. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Assante. Very practical and constructive recommendations.

Dean Turner is our next witness, Director of the Global Intelligence Network at Symantec Security Response, Symantec Corporation. Thank you for being here.

TESTIMONY OF DEAN TURNER,[1] DIRECTOR, GLOBAL INTELLIGENCE NETWORK, SYMANTEC SECURITY RESPONSE, SYMANTEC CORPORATION

Mr. TURNER. Thank you, Mr. Chairman and Ranking Member Collins. I would like to thank you for, of course, allowing us the opportunity to appear here today and to discuss not only the Stuxnet worm but how we can better begin to secure the industrial control systems that underpin this country's national critical infrastructure.

As you have pointed out, I am the Director of Symantec's Global Intelligence Network. As a leader in the security space, Symantec welcomes the opportunity to provide comments to the Committee as it continues its, arguably, important efforts to enhance the secu-

[1] The prepared statement of Mr. Turner appears in the Appendix on page 156.

rity of critical infrastructure systems from cyber attack. We believe that critical infrastructure protection is an essential element of a resilient and secure nation.

Let me begin by providing Symantec's observations on Stuxnet and offering our insights on the threat that the worm poses to this Nation's industrial control systems.

Symantec examined each of the Stuxnet components in order to better understand exactly how the threat worked in detail. We found Stuxnet to be an incredibly large and complex threat, and it is the first threat that Symantec has identified that targets critical industrial infrastructure and is written specifically to attack industrial control systems used in part to control and monitor industrial processes. Not only can Stuxnet successfully reprogram the programmable logic controllers (PLCs), that are part of these industrial control systems, but it also, as Mr. Assante and Mr. McGurk have pointed out, cleverly hides those modifications.

Stuxnet is able to accomplish this task via a rootkit, which is a type of malicious software that keeps itself hidden from the computer's operating system. Computer source code contained in the PLC is the function that allows control systems to operate and to control machinery in a plant or a factory. The ability to reprogram this function allows for the potential to control or alter how the system operates.

We speculate that the ultimate goal of Stuxnet is to reprogram and sabotage industrial control systems. The threat is targeting a specific industrial control system, and that is the one utilized by energy sectors, such as with a gas pipeline or power plant.

Stuxnet demonstrates the vulnerability of our critical infrastructure industrial control systems to attack and, again, as other witnesses' testimonies today have pointed out, highlights a problem and should serve as a wake-up call for our critical infrastructure systems around the world.

The potential for attackers to gain control of critical infrastructure assets, such as power plants, dams, and chemical facilities, is extremely serious. Whether Stuxnet ushers in a new generation of malicious code attacks toward critical infrastructure remains to be seen. Stuxnet is of such complexity—requiring significant resources to develop—that only a select few attackers are capable of producing such a threat. So we do not expect masses of similar sophisticated threats to suddenly appear.

Stuxnet does, however, highlight that attacks to control critical infrastructure are possible and not just a plot in a spy novel. The real-world implications of Stuxnet are some of the most serious that we have ever seen in a threat.

The intended target of Stuxnet is not known. We know even less about who could have written Stuxnet than the target itself. What we do know is that whoever was behind it has good knowledge of ICS systems, particularly those systems that were targeted. Without better knowledge of the persons behind these attacks, it is nearly impossible to say with any certainty who was ultimately responsible and what were the possible motives behind the attack. The combination of sophisticated attacker and their target means that any speculation as to who was behind that is just that: Speculation.

Symantec believes that education and awareness is a key component to securing critical systems from cyber attack. From the classroom to the boardroom, from the management level to the security professional, education is needed to ensure security is part of an organization's ethos. Good security requires secure software and well-designed and maintained networks. In other words, security needs to be baked in from the outset, and part of this is ensuring that all of those involved continuously maintain their skill sets in what is arguably a fast-changing environment.

The question being asked now of security professionals associated with U.S. critical infrastructure is what we should be doing in response to this particular discovery.

The first obvious measures to protecting these types of systems from Stuxnet and similar threats is to deploy up-to-date anti-malware solutions. Unfortunately, many industrial control systems today still need to be modernized in order to be able to do just that.

The second most important element is to watch for vendor security notifications and alerts and apply patches as soon as possible.

Last, but certainly not least, is know your assets, identify your perimeter of security operations, and maintain a high level of situational awareness to ensure you are aware of and can respond to these types of incidents in a timely manner.

Keeping in mind that over 85 percent of the U.S. critical infrastructure is owned and/or operated by the private sector, Symantec commissioned a recent study on critical infrastructure protection. Our goal here was to find out how aware critical infrastructure companies were of government efforts in this area and to determine how engaged business was about working government. And we came up with four key findings from that particular survey.

One, critical infrastructure providers are increasingly attacked.

Two, attacks on critical infrastructure are effective and costly.

Three, industry wants to partner with government on critical infrastructure protection.

And finally, fourth, critical infrastructure providers feel more readiness is needed to counter these types of attacks.

Most telling was that respondents cited security training, awareness by executive management of serious threats, endpoint security measures, security response, and security audits as the major safeguard areas in need of the most improvement.

Since most of the Nation's cyber infrastructure is not government owned, a public-private partnership of government and private stakeholders is required to secure the Internet and ICS systems. Cooperation is needed now more than ever, given that industrial control systems face an ever-increasing risk due to cyber threats such as Stuxnet.

Toward that end, Symantec commends the Department of Homeland Security for their engagement with the private sector on critical infrastructure protection. DHS has been a valuable partner to Symantec and others in the private sector, through the Sector Coordinating Councils as well as the IT Information Sharing and Analysis Center.

Symantec has provided input to DHS on the Comprehensive National Cyber Initiative projects, and we have been engaged with the Department on the National Cyber Incident Response Plan. Additionally, we participated in the National Cyber Exercise, Cyber Storm III, which demonstrated the value of operational incident collaboration across the public and private sectors. Further, we have held several briefings with DHS to share our expertise on Stuxnet and how critical infrastructures can better secure their systems against these threats. We look forward to continuing to partner with DHS and other agencies on the many issues and preparedness activities related to the Nation's critical infrastructure protection.

Stuxnet demonstrates the importance of public-private information-sharing partnerships across the entire critical infrastructure community. While DHS has made strides to partner with control system vendors through its ICS-CERT, it should build on its 2009 "Strategy for Securing Control Systems" and enhance its control systems partnerships by including the IT and IT security communities, who have traditionally worked with the DHS U.S. Computer Emergency Readiness Team (US-CERT). Cross-collaboration within DHS is the key to improved situational awareness and operational response, and DHS should continue its efforts to integrate these functions.

Until there is greater coordination between IT and IT security vendors and the industrial control systems owners and operators, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to learn from and collectively respond to threats. We recommend that DHS further enhance information sharing on control systems vulnerabilities with the IT and IT security communities and continue to work on integrating its information-sharing capabilities to improve situational awareness and operational response partnerships with industry.

In closing, Symantec would like to convey our strong support for the Protecting Cyberspace as a National Asset Act. We believe that this important legislation will enhance and modernize the Nation's overall cyber security posture in order to safeguard the critical infrastructure from attack. The bill also importantly recognizes cyber security as a shared government and private sector responsibility, one which requires a coordinated strategy to detect, report, and mitigate cyber incidents. We look forward to working with the Committee to help advance this important legislation.

Thank you for the opportunity to testify today. We remain committed to continuing to work in coordination with Congress, the administration, and our private sector partners to secure our Nation's critical infrastructure from cyber attack. And I will be happy to respond to any questions the Committee may have.

Chairman LIEBERMAN. Thanks very much, Mr. Turner. Thanks for your specific explicit endorsement of the legislation, which Senator Collins and I introduced and which the Committee reported out unanimously, obviously across party lines, and really thank you for the fact that your entire statement was really an explanation, in a sense a call to action for us to pass such legislation and to create a public-private alliance here to protect our country from this very serious threat.

Mark Gandy is our last witness. He is the Global Manager of Information Technology Security and Information Asset Management at the Dow Corning Corporation. Thank you for being here.

TESTIMONY OF MARK W. GANDY,[1] GLOBAL MANAGER, INFORMATION TECHNOLOGY SECURITY AND INFORMATION ASSET MANAGEMENT, DOW CORNING CORPORATION

Mr. GANDY. Thank you. Good morning, Chairman Lieberman, Ranking Member Collins, and Members of the Senate Homeland Security Committee. My name is Mark Gandy, and I am the Global Manager of Cybersecurity for the Dow Corning Corporation. I am also Chairman of the American Chemistry Council's Cybersecurity Steering Committee.

To begin, I would like to thank the Committee for holding this important hearing today on the critical issue of cyber security. While I realize this is not a legislative hearing, I would like to commend your efforts in crafting bipartisan legislation during this Congress that effectively balances the need for increased vigilance through the promotion of a risk-based framework whereby the critical infrastructure sectors can appropriately address their cyber threats.

The American Chemistry Council (ACC) and its members stand ready to support a continued momentum on this issue as we proceed into the next Congress. Today I will be making comments or statements on behalf of the American Chemistry Council.

The ACC represents the leading chemical companies in the United States. The business of chemistry is a critical aspect of our Nation's economy, employing more than 800,000 Americans and producing more than 19 percent of the world's chemical products. In fact, more than 96 percent of all manufactured goods are directly touched by the business of chemistry.

Cyber security is a top priority for ACC and the chemical sector. Because of our critical role in the economy and our commitments to our communities, security is a top priority for ACC members.

In 2001, our members voluntarily adopted an aggressive security program—the Responsible Care Security Code (RCSC)—which is mandatory for all members of the ACC. The RCSC is a comprehensive security management program that addresses both physical and cyber security and requires a comprehensive assessment of security vulnerabilities and risks and to implement protective measures across a company's entire value chain. Each company's security plan is then reviewed by an independent third-party auditor. The RCSC has been a model for State-level chemical security regulatory programs in New Jersey, New York, and Maryland and was deemed equivalent to the U.S. Coast Guard's Maritime Transportation Security Act.

Public-private partnerships are vital to winning the war on cyber terrorism. The ACC and its members have been proactively engaged with the former and current administrations on improving cyber security. In June 2002, ACC members began implementation of the Chemical Sector Cybersecurity Strategy, which was referenced by the Bush Administration's National Strategy to Secure Cyber Space of 2003. ACC participated in the White House 60-day cyber policy review, and our cyber experts work closely with the DHS National Cybersecurity Division in many areas, including national Cyber Storm exercises, information-sharing programs, and

[1] The prepared statement of Mr. Gandy appears in the Appendix on page 165.

development and implementation of the road map to securing control systems in the chemical sector.

ACC was gratified that in 2009 the Obama Administration made cyber security a top priority. A 2009 program update can be found on the Obama Administration's Web site, "Making Strides to Improve Cybersecurity in the Chemical Sector."

Since 2001, ACC members have invested more than $8 billion in your enhancements, including both physical and cyber security protections. Security in all its dimensions continues to be a top priority for ACC and the chemical industry, and our record of accomplishment and cooperation with Congress, DHS, and others is undisputed.

Considering the industry's perspective on the increased threat, we have seen the threat landscape evolve from relatively unorganized, unsophisticated exploits of virus and worm activity with a notoriety objective—making a name for the hacker—to increasingly more sophisticated and economically disruptive attacks to network computing into today's relatively sophisticated and stealthy threats that target intellectual property for economic gain and are potentially disruptive to operational stability of critical infrastructure.

However, while the threat landscape is evolving in sophistication and intent, many vulnerabilities exploited remain relatively unsophisticated, whereby well-known counter measures are possible. Cyber threats to control systems are evolving in complexity and sophistication as well-funded and highly motivated groups become more active. Specifically, Stuxnet is more advanced with respect to a targeted control system attack by a knowledgeable subject matter expert using typical technology exploits of common vulnerabilities inherent in any system. Stuxnet demonstrates that threats to process control systems are real and need to be a significant part of the cyber security risk management equation.

The industry recognizes the vulnerabilities of industrial control systems as they have increasingly become enterprise network connected. The threat is serious and the industry is responding by increased preparation and response planning with significant resources.

In response to the evolving threat landscape and the relatively commonly avoidable exploits, the industry is working proactively to improve information sharing among the industry and with government about threats, working with technology suppliers and the U.S. Government to enhance the robustness of control systems through the development of international standards for improved security of control systems, and developing and publishing risk management best practices and security guidance that help owner-operators better prepare and respond to cyber threats such as Stuxnet.

The industry approach is a comprehensive risk management strategy that includes proactive steps through ACC and the U.S. Government, emphasizing the importance of effectiveness threat and best practice information sharing and robust technology solutions. Our sector is also leading the development of comprehensive international standards by the International Society for Automation. These standards will lead to the development of control systems that are more resilient to cyber attacks.

ACC and its members are also actively engaged in the road map to secure control systems in the chemical sector along with our active partnerships with DHS and the Chemical Sector Coordinating Council. These and other activities make up a coordinated comprehensive sector program that was significantly informed through participation in exercises such as the recently completed Cyber Storm III.

In summary, the ACC and its members remain committed to advancing cyber security practices and systems in the chemical industry by working in partnership with Congress, DHS, technology organizations, and developers. Working with the chemical sector at large, we are improving how we share information and striving for continuous improvement of critical control systems that are protected from the loss of critical function during a major cyber event.

The Federal Government plays a crucial role in helping the sector to achieve this goal by creating and supporting programs and incentives that promote advances in new technologies and standards and upgrading of legacy systems across the sector.

Sharing of timely and actionable threat information with the private sector and working together on risk-based solutions that focus on the resiliency of control systems should be an area of heightened attention and focus to mitigate the evolving threats.

And, last, identifying and holding accountable those who attack our critical cyber infrastructure, whether it is for notoriety or for financial gain, must be a priority.

That concludes my opening statement. We have submitted a written statement for the record. Thank you for this opportunity to present on behalf of the ACC, and I will be happy to take any questions that you have. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Gandy. Encouraging to hear that private sector response to the growing threat, and your statement, along with others, will be entered into the record.

I want to just formally welcome Senator Coons for the first time. He was sworn in 2 days ago as the new Senator from Delaware. There is a great tradition of Delaware Senators serving on this Committee. I know you bring extraordinary experience and ability, and we look forward to working with you on the Committee.

Senator COONS. Thank you, Mr. Chairman.

Senator COLLINS. Let me join the Chairman in also welcoming Senator Coons to our Committee. As he mentioned, I think there has been a Senator from Delaware on this Committee going back to Bill Roth's days for decades.

Chairman LIEBERMAN. Bill Roth, right.

Senator COLLINS. And we are delighted to have you join us and hope it will be a permanent assignment. I know that is still up in the air. Thank you.

Chairman LIEBERMAN. Me, too. Thanks, Senator Collins.

I think we will do 6-minute rounds here so we can try to give everybody an opportunity in case the vote actually goes off on time at 11 a.m.

This has been excellent testimony, and what it reminds me of, obviously, as a lay person, if you will, here, is that cyberspace is a lot different from the normal space we occupy, even in terms of what we are describing as the threat. I think you, Mr. Turner, said something so interesting, which is we really do not know who the attacker was in the Stuxnet case. That I can understand because of all the difficulty. But what is fascinating is that—and I believe I understand this—we do not know what the target was either. But we know that there was a Stuxnet attack and that it is real.

So, Mr. McGurk, maybe I will start with you on this to help our education because my understanding is—and I say this with pride—that the Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team, which we call more simply ICS-CERT, played a critical role in unraveling Stuxnet. So help us understand a little more what this thing is, whose origin and destination we do not understand.

Mr. McGurk. Yes, Senator. Thank you for that opportunity. As you had mentioned, the ICS-CERT took the initial focus of analyzing what the capabilities of Stuxnet were. In order to understand its code, we identified by reverse engineering the physical attributes of the code and how it actually exploited the information technology vulnerabilities. There were these undocumented capabilities in the operating system, which are often called "zero day" vulnerabilities. They are called "zero day" because no one knows about them.

In this particular case, this code utilized four zero day vulnerabilities to ensure that the malicious part that affects the industrial control system was delivered. So using a device such as the USB device, it actually migrated through the networks and then went into the physical process control environment. We were able to take the equipment at our laboratory out at Idaho National Labs and physically configure it with representatives from the vendor community themselves. The actual vendors of the products came out and helped configure the equipment, and then we actually allowed Stuxnet to go loose into the environment, if you will.

Because it was written with such advanced cryptological and obfuscation technologies, Stuxnet actually used the equipment itself that it was attacking to encode itself. So we were able to actually give it that programmable logic controller that it was looking for because it focuses on a specific hardware and software combination, and actually it was able to dissect the code by accessing the programmable logic controller, and it started decrypting itself. That allowed us to speed our analysis along, and it did not take as much time to identify not how it was written but what it was capable of doing.

Our focus was on developing and understanding its capabilities and then identifying those mitigation strategies. So our efforts allowed us to do that.

Chairman Lieberman. So where was it found? I am thinking in conventional terms, but this thing that you analyzed, whose origin and destination was not clear, nonetheless had to exist somewhere so you could analyze it.

Mr. McGurk. The first sample of code that we received was actually working in our partnership with various international CERTs. We received it from the German CERT, who in turn received it from the vendor themselves.

Chairman Lieberman. The vendor was a Germany company?

Mr. McGURK. It was a German company; yes, sir. So, subsequently, we were able to get a pure sample of the code that was in the wild, and that allowed us to conduct that reverse analysis.

Chairman LIEBERMAN. And the control system targeted here, as I think one of you said, was a control system that is usually used for the control of power plants? Is that right?

Mr. McGURK. Essentially, these devices are ubiquitous. This particular vendor has a market share of about 7 percent here in the United States. There are other companies that have larger percentages. But these particular pieces of equipment are used in agriculture, manufacturing, power generation, water treatment, several sectors across the United States. Power generation and distribution is only one of those and not necessarily in this particular case the largest. Manufacturing is actually the larger infrastructure that uses these types of systems.

Chairman LIEBERMAN. In terms of the origin of it, although I understand we do not conclusively know, I presume—do we think that this was a Nation state actor and that there are a limited number of Nation states that have such advanced capability?

Mr. McGURK. Nothing in the code really points to any specific sense of origin or where it was developed. Based on our analysis, we feel that it was probably developed over a set period of time. These individual blocks were put together by a team or a series of teams working in concert, because there are indicators that it was strung together in such a fashion. But we have also identified with other types of malicious code and botnets where they actually generate $30 million a month in revenue from operating as various botnets. So when you have that capability from a criminal intent standpoint, you have resources to be able to buy this type of capability.

Chairman LIEBERMAN. There has been some speculation in the media that the target here might have been the nuclear power systems within Iran. In fact, at one point—perhaps unrelated to Stuxnet—an Iranian official complained about the fact that their nuclear program was under cyber attack, not linking these two. What would you say in response to that?

Mr. McGURK. Again, sir, attribution and intent are the fields for other departments and agencies. We are focusing primarily on capability. But I would also like to also acknowledge Mr. Turner's comments that there would be an incredible amount of knowledge necessary to be able to identify specifically what the target was, and there are no indicators in the code. We understand what it is capable of doing.

Chairman LIEBERMAN. Right.

Mr. McGURK. But to specifically say it was designed to target a particular facility is very difficult for anyone to say with any assurance.

Chairman LIEBERMAN. Thank you. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Turner reminded all of us that 85 percent of critical infrastructure is in the private sector, and that is why the bill that the Chairman and I drafted focuses on public-private partnerships and information sharing that is absolutely critical. I would like to ask each of you to comment on two issues related to that.

First, how vulnerable is our Nation's critical infrastructure to cyber threats like Stuxnet? And then, second, how would you characterize the level of preparedness in the private sector to deal with a threat of this sophistication?

We will start with you, Mr. McGurk, and just go down the table. Thank you.

Mr. MCGURK. Thank you, Senator. As far as how vulnerable, I think the issue was made clear earlier in many of the testimonies before the Committee that the advent and adoption of commercial off-the-shelf technology into a critical process environment has now opened each of those former legacy-based systems to the same types of vulnerabilities we have in information technology today. By connecting these systems and, if you will, systems of systems together, we have actually increased the risk profile associated with those networks and operating those networks.

The private sector has been working diligently to identify those mitigation strategies and those steps as they integrate that technology. The Department has been working in our private-public partnership capacity to provide the services and the expertise that we have to help identify those processes in securing the critical infrastructure.

It is an uphill battle, and when we see something like Stuxnet come into play that significantly alters the landscape, we need to reassess and re-evaluate our mitigation plans so that we can identify new methods of increasing that security, and the private sector working with the Department has been focusing on that for quite some time now.

Senator COLLINS. Thank you. Mr. Assante.

Mr. ASSANTE. I think it is important to note that in my time at NERC and working with the industry, there were lots of incidents where we had non-directed and not very structured cyber threats that impacted or found their ways onto control systems. That was very concerning because it was not by design. It found its way because technology is very cross-cutting. That indicates to me that we are not only very susceptible, but not very well prepared since we had architectures that allowed for that to happen.

When you look at the Stuxnet worm, you are talking about a very well resourced and very structured cyber adversary with advance planning capability. In that sense, I believe we are extremely susceptible. In fact, I believe our susceptibility grows every day. If you just look at the very trends within the technologies that we deploy, we are doing things that would allow an attacker more freedom of action within these environments.

As an example, we are converging safety systems with control systems at the network layer. It is a very dangerous combination because you allow somebody to get free access to both the system that is designed to make sure a process stays safe and the system that controls what a process does. Those types of trends that our manufacturers, vendors, and even our asset owners have called for because there is great business efficiencies to do are very dangerous and troublesome. So I believe we are becoming more susceptible to these types of attacks every day.

Senator COLLINS. Thank you. Mr. Turner.

Mr. TURNER. Senator Collins, I concur with Mr. McGurk and Mr. Assante, to the level of complexity in the issues that we are facing today. In my role within Symantec, I spent a good deal of time looking at vulnerabilities and talking about numbers and trends and threats and all the rest of it. And I think what I would like to do is maybe illustrate using Stuxnet just exactly where we stand.

As of early last week, we saw approximately 44,000 unique Stuxnet infections worldwide. Now, that may not sound like a big number, but when we are talking about a highly sophisticated threat that requires an awful lot of knowledge and skills and people to pull together, that is a big number.

In terms of the United States, we have seen a little over 1,600 unique Stuxnet infections, 50 of which we have identified as having the WinCC/Step7 Stuxnet—the software that Stuxnet trojans installed. Sixty percent of the global infections of Stuxnet are in Iran. And we can talk about speculation and all those other things about where the evidence points, but the point here is that even if something like this is tied to one particular country or group of countries, the ability for these types of threats to have a global reach is enormous. We have gone from the days, in 2004, where we saw a little over 260,000 new threats to where we saw 2.9 million last year. Vulnerabilities in software and hardware have become, unfortunately, in some ways a cost of doing business. There is an awful lot of issues here.

Our level of preparedness, I think, is to some degree, certainly in the private sector, better than it ever has been, but still has a long way to go. It is a cliche, but unfortunately, we do not know what we do not know. And when we start talking about industrial control systems and some of the other things where the partnership is not quite as developed as it should be, it is a little more difficult to answer.

So how vulnerable are the industrial control systems and supervisory control and data acquisition (SCADA) systems within the United States or anywhere else? That is a difficult question to answer until we know exactly the scope of the problem and how many vulnerabilities there are.

Senator COLLINS. Thank you. Mr. Gandy.

Mr. GANDY. Regarding the vulnerability question, the chemical sector understands this evolving threat, has been working proactively to ensure the resiliency of our control systems from both the physical and cyber approach through a risk-based framework that identifies these vulnerabilities and then works on implementing appropriate mitigating controls. As mentioned, the Responsible Care Security Code, the road map to securing control systems in the chemical sector, ongoing Chemical Facility Anti-Terrorism Standards (CFATS) compliance work, are all working to comprehensively provide a framework of assessment, design, engineering, implementation, and monitoring for these kinds of vulnerabilities.

The level of preparedness in the sector, the ACC and its members have been working for years across the sector to prepare and share information about these issues, both from an industry peer-to-peer sharing and sharing with technology suppliers and DHS and national cyber information-sharing exercises. We continue to comprehensively improve control system security in the chemical sector.

The road map to security in the control system in the chemical sector is further driving the resiliency of control systems through preparedness and awareness.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Coons.

OPENING STATEMENT OF SENATOR COONS

Senator COONS. Thank you, Mr. Chairman, for holding these interesting and important hearings.

If I might, Mr. Gandy, I just want to commend the ACC for its model private sector initiative.

For the whole panel, one of the things that made Stuxnet, I think, particularly concerning is its ability to both infiltrate and then exfiltrate data that are operational in nature and would allow an unknown observer to then map an industrial process. What sort of risks does this pose for trade secrets in the event that we have foreign nations who are competitors to this country interested in using this kind of capability to learn about detailed operational configuration of our manufacturing processes, our power grid, our chemical processes in a way that would allow them to then mimic them, map them, and expand them, or make them strong?

So I would be interested, if I could, in brief answers from all the members of the panel to two questions. Does Stuxnet signal not just a risk in terms of infrastructure but also intellectual property and the potential loss of American trade secrets? And then, second, what could we be doing to strengthen the public-private partnership on both fronts, both the intellectual property and the operational control of critical infrastructure? If we could start with Mr. McGurk. Thank you.

Mr. MCGURK. Thank you, Senator. To answer the question succinctly, yes, it does demonstrate the very unique capability of exfiltrating or removing that data associated with critical process development. In addition, it has an advanced capability that we have seen demonstrated where it can actually remove the historical files associated with the process. That is a key element because it actually goes into development and refinement of your process, so I know not only what you are currently producing but what you have produced in the past and what changes you have made to refine that process. So, subsequently, from an intellectual property standpoint, it poses a very great risk.

In order to strengthen that partnership, I think we are all discussing the very same topic of awareness and understanding and putting those mechanisms in place, whether it is through education, certification, or through information sharing, and actually collaborative development of information in order to address risks such as Stuxnet. Thank you, sir.

Senator COONS. Thank you.

Mr. ASSANTE. I think the Stuxnet worm was very sophisticated and capable and that not only did it allow you to maintain a foothold in the environment that you compromise, which is what the attacker wants to do, through the exportation of information it allows them to conduct discovery. Discovery is a very important element to being able to plan follow-on attacks, if that is what the author would so choose to do. And so whether discovery is by pulling out information that has value or that has information that would support future planning processes or the ability to just recognize how you maintain a sustained foothold, that is a very significant issue for the industrial control system world, and certainly we have seen that play out in threats across financial services, defense industrial base, and other key sectors of our economy where we have trade secrets or proprietary information that is important to our economic stability.

I do not want to gloss over the idea that the Stuxnet worm was so sophisticated that it was capable of acting autonomously. So whether they lost that communication link, that piece of code had quite a bit of intelligence to be able to act. So I think the concept of follow-on attack is important.

I believe from the public-private partnership perspective, I have seen great progress. I have been involved in it over the years. I do believe that the proposed legislation that this Committee is looking at which be a significant step forward to further ingraining how we should go about what I think is a more productive partnership. I think that we need to not only hold the asset owner responsible for the management of risk as it relates to the systems that they manage, but also the technology providers. We will constantly be trying to be very reactive if we do not get the technology providers to take a serious part in being able to program these systems more securely, to help design the architectures, they will be better suited to deal with these types of advanced threats.

Mr. TURNER. Senator Coons, echoing the comments by Mr. Assante and Mr. McGurk, the short answer is yes, absolutely it is a risk. Ninety to 95 percent of all the threats we see today are risks to personally identifiable information. The fact that this is wrapped up into a threat that targets critical infrastructure is just as important as any other one, and more so in many ways.

We know, for example, that there was the capability before the sink holes—the command-and-control (CnC) servers were taken over by Symantec—that this particular code had the ability to actually install a back door on those systems. So the systems that we did not know about between June 2009 and where we are today in 2010 could still be exfiltrating data. We know that part of the threat's purpose was to steal the design documents of the ICS systems. That particular information could still be leaked.

We do need to take this seriously because it is all about information—the secondary component, of course, being what could you do not only with that information, but more importantly changing the frequency control that drives themselves and all the other things that could take place.

I think in terms of what do we need to do to strengthen our partnerships, there is a fair amount of activity taking place in back channels where security experts are discussing the issues and the threats amongst themselves and also coordination among the organizations. Organizations like TechAmerica have undertaken industry working groups where we get together and we discuss better ways to share information, not only between ourselves but between government and the rest. And I think that is also a very important step forward, in addition to, obviously, the legislation that is proposed by the Committee.

Senator COONS. Thank you.

Mr. GANDY. Senator Coons, yes, we believe, the industry believes that intellectual property is a target of these malware writers. The intentions of Stuxnet, aside, we believe malware will be on our enterprise business networks and on our process control networks that will attempt to comprehensively steal our intellectual property, reverse engineering our processes, and stealing other sensitive business information.

Regarding what can we be doing more from a public-private partnership, we continue to believe that continued working groups, such as the Industrial Control Systems Joint Working Group, are essential to the government, industry, and the suppliers working together to work on the resiliencies of control system security. We also continue to encourage participation in national exercises such as the Cyber Storms so that we can continue to work on information sharing, continue to practice information sharing, identify road blocks, improve the efficiency, effectiveness, and timeliness of the information that is shared.

Senator COONS. Thank you very much to the panel, and thank you, Mr. Chairman, for the opportunity to ask questions.

Chairman LIEBERMAN. Thank you, Senator. I appreciate it.

The votes have gone off. I think rather than holding you here and coming back, I will try to ask a few more questions and see if I can hustle over before the votes are done.

I want to get clear—I think it was you, Mr. Turner, who said that 60 percent of computers infected with Stuxnet are in Iran.

Mr. TURNER. That is correct. Sixty percent of the infections that we have observed worldwide are coming from Internet Protocol (IP) addresses of machines identified as being in Iran.

Chairman LIEBERMAN. And have we identified any computers infected in the United States?

Mr. TURNER. We have.

Chairman LIEBERMAN. Just as a natural movement of the Stuxnet, or is it also a unique——

Mr. TURNER. Well, intent is one of the hardest things to determine, Mr. Chairman. This particular threat and the way it first propagated was via a USB device, taking advantage of a particular vulnerability in Microsoft, something known as ".lnk." So in order for something like that to propagate to get over to the United States, a USB drive would have to get on a plane. But that does not mean, of course, that the particular code could not be transferred from one person to another.

Chairman LIEBERMAN. Right.

Mr. TURNER. We think that most of the infections we see worldwide are anecdotal and antecedent to the originals.

Chairman LIEBERMAN. They have fed off the original.

Mr. TURNER. Correct.

Chairman LIEBERMAN. Understood. Mr. McGurk, we have heard you discuss the resources that DHS can provide for the private sector in this regard. These are resources that the private sector can choose to utilize or choose to ignore, correct?

Mr. MCGURK. Yes, that is correct, Senator. We only respond when requested by the private sector. We have no authorities to actually direct that activity.

Chairman LIEBERMAN. Right. So my question naturally is—and I would ask the others as well quickly—whether you believe that we can increase cyber security of our country's most critical infrastructure through voluntary measures alone. Or does the Department of Homeland Security in this case need some enhanced authority? Obviously, to state underneath that the whole premise of this hearing today and the focus on Stuxnet is both to educate the Committee, but also to say to us as the Homeland Security Committee, if this can be done to somebody else, obviously it now can be done to us, so we better raise our guard.

So let me come back to the question. Can we do what we have to do by voluntary measures? Or does DHS need some kind of enhanced authority? Mr. McGurk.

Mr. MCGURK. Again, Senator, I appreciate the opportunity to reply to that. I am a simple sailor, 28 years in the Navy. I am used to executing and operating my orders under the authorities that are granted to me. The Department has policy decisionmakers in place that actually identify those requirements. My focus is on managing and leading the operational environment that I am entrusted with at the Department. And given those responsibilities, we have been operating within those guidelines. And for the most part, we have not been as successful as we could potentially be, but we are as successful as we can be within those guidelines.

Chairman LIEBERMAN. So you would accept enhanced authority if we gave it to you, but you are not appealing for it right now? [Laughter.]

Mr. MCGURK. Sir, I feel confident that I am still able to execute the current mission given the requirements.

Chairman LIEBERMAN. Mr. Assante.

Mr. ASSANTE. Well, as a fellow Navy shipmate, Mr. McGurk, I believe that DHS and the U.S. Government would benefit from additional authorities in this area. I believe it is critical that organizations cannot suffer in silence. If an advanced threat is on our shores impacting our systems, that should be a required thing to report. We should be able to muster the effective resources that we have, whether it is in government or within industry, to be able to tackle those and very rapidly share information so we can protect our systems. I think advance authority would allow us to do so.

I believe participating in regulation in the electric power industry, you get to be very smart in how you design the regulation and the legislation. Performance requirements are very important in my book. I think there are some unsafe practices that we continue to use that we need to ensure that they are curtailed. And I think that we need to maximize our ability to learn and still be able to innovate. So I think authority is necessary.

Chairman LIEBERMAN. Thank you.

Mr. Turner, my time is running out, but see if you can give a quick answer, the same to Mr. Gandy.

Mr. TURNER. I think that more time and effort needs to be spent in shoring up the current channels of communication between all parties involved in the discussion. There are, of course, very tricky legal and ethical issues around certain types of data that might be personally identifiable information (PII) and the rest of it, because it is not just data that occurs in the United States of America but data that occurs elsewhere in the world.

Chairman LIEBERMAN. Right.

Mr. TURNER. And if the goal is to get as much information as possible into the hands of the people who can do the most to take care of the issue, the best way to do that is to actually strengthen the channels of communication that currently exist.

Chairman LIEBERMAN. Mr. Gandy, the chemical industry, as you well know, is actually subject now under other legislation to risk-based performance requirements similar to those contemplated in our legislation. What do you think?

Mr. GANDY. That is correct. My response would be that I believe there is evidence that the industry is already working voluntarily, very productively, and the CFATS work that is ongoing right now where DHS is out reviewing the registered most critical sites of the critical infrastructure in the chemical sector against those risk-based performance standards will help us continue to improve our security posture in the face of this threat.

Chairman LIEBERMAN. Thank you. We have covered a lot more ground, I might say, in this period of time than the Committee usually does, and it is because not only we were rushed, but because of the quality of the witnesses. I cannot thank you enough.

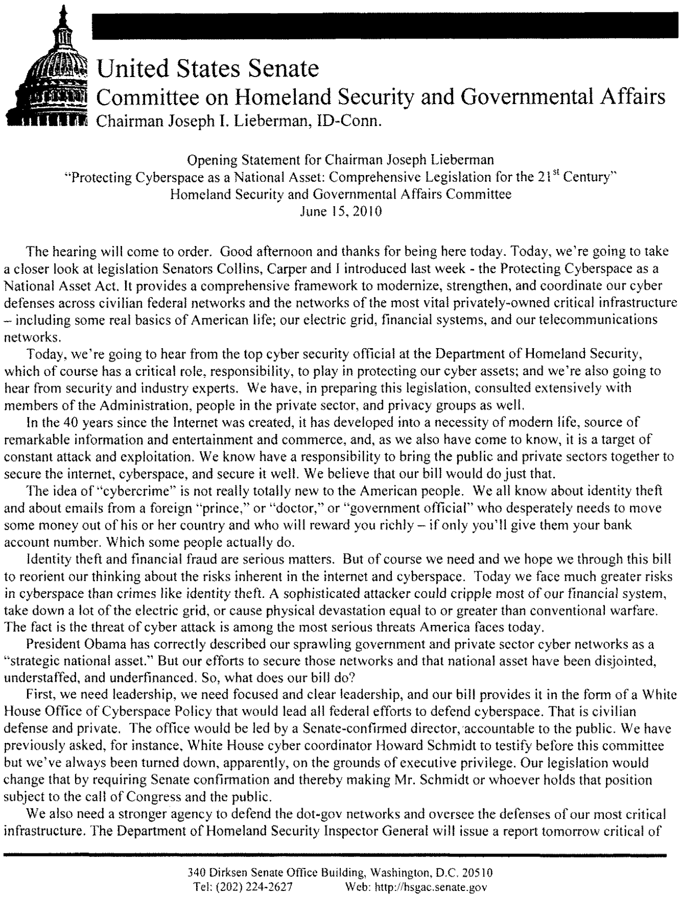
I want to restate that this Committee is going to make our cyber security legislation or legislation like it a priority early in the next session, beginning in January.

We are going to keep the record of this hearing open for 15 days for additional questions and statements, but I thank you very much for what you have done today and for the work you are doing to protect our country every day.

The hearing is adjourned.

[Whereupon, at 11:22 a.m., the Committee was adjourned.]

APPENDIX



United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement for Chairman Joseph Lieberman
"Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century"
Homeland Security and Governmental Affairs Committee
June 15, 2010

The hearing will come to order. Good afternoon and thanks for being here today. Today, we're going to take a closer look at legislation Senators Collins, Carper and I introduced last week - the Protecting Cyberspace as a National Asset Act. It provides a comprehensive framework to modernize, strengthen, and coordinate our cyber defenses across civilian federal networks and the networks of the most vital privately-owned critical infrastructure – including some real basics of American life; our electric grid, financial systems, and our telecommunications networks.

Today, we're going to hear from the top cyber security official at the Department of Homeland Security, which of course has a critical role, responsibility, to play in protecting our cyber assets; and we're also going to hear from security and industry experts. We have, in preparing this legislation, consulted extensively with members of the Administration, people in the private sector, and privacy groups as well.

In the 40 years since the Internet was created, it has developed into a necessity of modern life, source of remarkable information and entertainment and commerce, and, as we also have come to know, it is a target of constant attack and exploitation. We know have a responsibility to bring the public and private sectors together to secure the internet, cyberspace, and secure it well. We believe that our bill would do just that.

The idea of "cybercrime" is not really totally new to the American people. We all know about identity theft and about emails from a foreign "prince," or "doctor," or "government official" who desperately needs to move some money out of his or her country and who will reward you richly – if only you'll give them your bank account number. Which some people actually do.

Identity theft and financial fraud are serious matters. But of course we need and we hope we through this bill to reorient our thinking about the risks inherent in the internet and cyberspace. Today we face much greater risks in cyberspace than crimes like identity theft. A sophisticated attacker could cripple most of our financial system, take down a lot of the electric grid, or cause physical devastation equal to or greater than conventional warfare. The fact is the threat of cyber attack is among the most serious threats America faces today.

President Obama has correctly described our sprawling government and private sector cyber networks as a "strategic national asset." But our efforts to secure those networks and that national asset have been disjointed, understaffed, and underfinanced. So, what does our bill do?

First, we need leadership, we need focused and clear leadership, and our bill provides it in the form of a White House Office of Cyberspace Policy that would lead all federal efforts to defend cyberspace. That is civilian defense and private. The office would be led by a Senate-confirmed director, accountable to the public. We have previously asked, for instance, White House cyber coordinator Howard Schmidt to testify before this committee but we've always been turned down, apparently, on the grounds of executive privilege. Our legislation would change that by requiring Senate confirmation and thereby making Mr. Schmidt or whoever holds that position subject to the call of Congress and the public.

We also need a stronger agency to defend the dot-gov networks and oversee the defenses of our most critical infrastructure. The Department of Homeland Security Inspector General will issue a report tomorrow critical of many operational elements of the Department's cybersecurity effort, citing a lack of clear authority as one of the issues that needs to be rectified. Our bill more than addresses these shortcomings by creating a National Center for Cybersecurity and Communications within the Department of Homeland Security which would have new, strong authorities to protect non-defense, public sector and private sector networks from cyber attack. DHS already has this responsibility through presidential directive, but, in our opinion, insufficient authority to carry it out.

The sound defense of our cyber networks will only be successful if industry and government work together, so our bill will set up a collaborative process where the best ideas of the private sector and the government would be used to meet a baseline set of security requirements that DHS would enforce for the nation's most critical infrastructure.

Thanks to some excellent work by our colleague Senator Carper, our legislation reforms and updates the Federal Information Security Management Act to require continuous monitoring and protection of federal networks but do away with the paper-based reporting system that takes up time agencies really otherwise would be using and should be using to protect their networks.

Our legislation also would require the federal government to develop and implement a strategy to ensure that the almost $80 billion of information technology products and services that the federal government purchases each year--$80 billion--are secure and don't provide our adversaries with a backdoor into our networks. And of course if the federal government uses that $80 billion of purchasing power to drive security add-ons and innovations in information technology products it'll also be available and presumably bought by the private sector.

Finally, we would give special authority to the President to act in the event of a catastrophic cyber attack that could seriously jeopardize public safety or have disastrous effects on our economy or national security. In those instances, clearly defined in our legislation, the President could direct the National Cybersecurity and Communications Center at DHS to impose emergency measures on a select group of critical infrastructure to preserve those assets and the networks they rely on and protect the American people. These emergency measures would automatically expire within 30 days unless the President ordered an extension. I know there's been some concern and controversy about that provision and we can speak to it I hope in the question and answer period. But it's very important limitation on liability of private entities who take action in response to an order from the government and might otherwise incur liability. We protect them from that because the action the government is ordering them to take is in national security or economic interest.

So, freedom of expression and freedom to innovate are not inconsistent with greater security in cyberspace and that is exactly what we hope to combine and balance in this legislation.

Senator Collins.

Opening Statement of
Senator Susan M. Collins

"Protecting Cyberspace as a National Asset Act of 2010"

Committee on Homeland Security and Governmental Affairs

June 15, 2010

★ ★ ★

The information revolution touches every aspect of our lives, from personal relationships and entertainment to commerce and national security information. Cyberspace is a place of great, even unparalleled, power, but also of great vulnerability.

Cyberspace is under increasing assault on all fronts. The cyber threat is real, and the consequences of a major successful national cyber attack could be devastating. As former Director of National Intelligence Michael McConnell testified in February, "If we went to war today, in a cyber war, we would lose."

Since the terrorist attacks of September 11, 2001, we have done much to protect potential targets such as ports, chemical facilities, and other vital assets. We cannot wait for a "cyber 9/11" before our government realizes the importance of protecting our cyber resources.

We are already under fire. Just this past March, the Senate's Sergeant at Arms reported that the computer systems of Congress and the Executive Branch agencies are now under cyber attack an average of 1.8 BILLION times per month. Cyber crime already costs our national economy an estimated $8 billion per year.

We must move forward now with an aggressive and comprehensive approach to protect cyberspace as a national asset. The vital legislation that we introduced last week would do just that, fortifying the government's efforts to safeguard America's cyber networks. It would build a true public/private partnership to promote national cyber security priorities.

For too long, our approach to cyber security has been disjointed and uncoordinated. This cannot continue. The United States requires a comprehensive cyber security strategy and strong coordination among law enforcement, intelligence agencies, the military, and the private owners and operators of critical infrastructure.

Our bill would establish an essential point of interagency policy coordination within the White House. The Office of Cyberspace Policy would be run by a Senate-confirmed Director who would advise the President. This Director would develop a national cyber security strategy.

To be clear, the White House official would not be another unaccountable czar. The Cyber Director would have defined responsibilities and be accountable to Congress. The Cyber Director would be an advisor and coordinator - not an implementer.

That responsibility, for federal civilian systems and private sector critical infrastructure, would fall to a strong operational and tactical partner at the Department of Homeland Security – the newly created National Center for Cybersecurity and Communications.

For its day-to-day operations, the Center would use the resources of DHS, and the Center Director would report directly to the Secretary of Homeland Security.

On matters related to the security of federal networks, the Director would regularly advise the President – a relationship similar to the Director of the NCTC on counterterrorism matters or the Chairman of the Joint Chiefs of Staff on military issues.

These dual relationships would give the Center Director sufficient rank and stature to interact effectively with the heads of other departments and agencies. These relationships would be critical for the Center Director to set, monitor compliance with, and enforce security policies for federal civilian systems.

As we have seen repeatedly, from the financial crisis to the environmental catastrophe in the Gulf of Mexico, what happens in the private sector does not always affect just the private sector. The ramifications for government and for the taxpayers often are enormous.

This bill would establish a public/private partnership to improve cyber security across private sector networks. Working collaboratively with the private sector, the Center would produce and share useful warning, analysis, and threat information with the private sector, other federal agencies, international partners, and state and local governments.

Best practices developed by the Center would be based on collaboration and information sharing with the private sector. Information shared with the Center by the private sector would be protected.

In cases where owners and operators are responsible for assets whose disruption would cost thousands of lives in mere seconds or multiple billions of dollars, the bill would establish certain risk-based performance requirements to close security gaps.

These requirements, for example, would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted.

These owners and operators would be able to choose which security measures to implement to meet applicable risk-based performance requirements. This model would allow for continued innovation that is fundamental to the success of the IT sector.

The bill also would provide limited liability protections to the owners and operators of covered critical infrastructure that comply with the new risk-based performance requirements.

If a cyber attack were imminent or occurring, the bill would authorize the President to undertake emergency measures to protect the nation's most critical infrastructure. The President would be required to notify Congress in advance of the declaration of a national cyber emergency, or as soon thereafter as possible. These emergency measures would be limited in duration and scope. The bill does not authorize any new surveillance authorities or permit the government to "take over" private networks.

The legislation also would take advantage of the federal government's massive purchasing power to help bring heightened cyber security standards to the marketplace.

Finally, the bill would improve the recruitment and retention of a qualified federal IT workforce.

If hackers can nearly bring Estonia to its knees through cyber attacks, infiltrate a major defense program, and hack the computers owned and operated by some of the world's most successful private sector computer experts, we must assume even more spectacular and potentially devastating attacks lie ahead.

I look forward to moving our bipartisan, comprehensive cyber security legislation forward this Congress.

Statement of Senator Thomas R. Carper

Committee on Homeland Security and Governmental Affairs

June 15, 2010

Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century

I want to start off my opening statement by thanking Chairman Lieberman and Ranking Member Collins for their leadership on this important national and economic security issue. This hearing to examine the various aspects of our comprehensive cyber security legislation is both timely and important.

As we all know, the Internet has certainly grown over the years – both in its complexity and in its impact on our everyday lives.

For the past three years, I have called for some of the very same reforms we will talk about today. In fact, I introduced cyber security legislation last spring in an effort to strengthen our Federal government – and our nation – against the kinds of attacks that we have seen seriously disrupt the nations of Estonia and Georgia.

One reform I am happy my colleagues accepted is the creation of a White House office that would be responsible for coordinating the security and resiliency of our nation's cyber space. To date, Federal agencies' efforts have been ad-hoc and duplicative. As the saying goes, the 'left hand didn't know what the right hand was doing.' My hope is that this office will provide the needed strategic direction to more effectively deal with challenges in cyberspace before they become a crisis.

Another reform I am happy made it into the bill is the idea that agencies need to leverage their purchasing power to demand private vendors sell more secure products and services. For too long agencies have needlessly spent money cleaning up after a cyber attack because the technology was full of security holes. Like a door with no lock, hackers have used security holes that never should have been there in the first place to gain access to our sensitive networks. Our bill changes that.

I also commend my colleagues for joining me in reforming the Federal Information Security Management Act of 2002. As we all know, producing a plan that sounds good on paper is not the same as ensuring the plan is effective when implemented. That's why our bill compels agencies to stop producing the reams of ineffective paperwork they currently do and instead focus their efforts on defending their systems in real-time.

Lastly, I thank my colleagues for accepting my language to create a nation-wide network of cyber challenges to help reduce the gap between the number of so-called "cyber warriors" that are produced in America and those being trained in China, North

Korea, and Russia. Like a "farm system" in baseball, these cyber challenges will create a pipeline of talent that can be tapped by government agencies and private sector companies. If we want America to continue to be dominant in the century to come, we must invest in the skills of our youngsters.

In closing, I look forward to working with Chairman Lieberman, Ranking Member Collins, and other Senate colleagues who may have interest in this issue. My hope is that we can bring together a diverse group of stakeholders on all sides of the issue to produce a bipartisan bill that will enhance our nation's cyber security and be signed by the President before the end of this year.

Statement for the Record
of
Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

June 15, 2010

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is an honor to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. I appreciate the opportunity to testify today regarding the critical issue of cybersecurity, and to discuss some of the major aspects of the Protecting Cyberspace as a National Asset Act.

The President has described our networks, and the hardware that supports them, as "strategic national assets" and called the growing number of attacks on these networks "one of the most serious economic and national security threats our nation faces." The President has also clearly laid out the roles and responsibilities for protecting nationally critical civilian networks:

- DHS has the lead to secure federal civilian systems, sometimes described as the dot-gov domain.
- DHS works with critical infrastructure and key resources (CIKR) owners and operators—whether private sector, state, or municipality-owned—to bolster their cyber security preparedness, risk mitigation, and incident response capabilities.

With that in mind, I would like to begin with a few key points.

- First, this cybersecurity endeavor is not just about DHS. The mission is for the entire homeland security enterprise, which includes many agencies, such as DHS, and the Departments of Commerce, State, Justice, and Defense. DHS will continue to play a critical role because of its responsibility to secure federal civilian networks and its mission to protect CIKR, both physical and cyber, in close coordination with the private sector and state governments but is actively engaged with its sister agencies on public policy and operational challenges that might impinge upon our nation's cybersecurity.
- Second, in response to the President's call to action a year ago, DHS has been focused on addressing an increasingly threatening cyber environment. We are fulfilling our mission responsibilities and challenging the status quo.

- Third, DHS is vigorously developing new capabilities, increasing response capacity, organizing for future successes, and bolstering security in both the public and private sectors.
- Fourth, there is no silver bullet to cybersecurity; we must employ a defense-in-depth approach. We are bringing in the technology and capabilities that the private sector has to offer, and we are encouraging and promoting innovation and creativity in order to achieve increased security and resiliency.

Mr. Chairman, the United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

As bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We can never be certain that our information infrastructure will remain accessible and reliable during a time of crisis, but we can reduce the risks.

We face persistent and unauthorized intrusions to federal executive branch civilian networks that often are difficult to attribute. These intruders may be nation state actors, terrorists, organized criminal groups, or individuals located here in the United States or abroad. They have varying levels of access and technical sophistication, but all have nefarious intent. Many are capable of targeting elements of the U.S. information infrastructure to disrupt, dismantle, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, and disruption of economic stability. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. Terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own technical abilities, of equal concern is the wide availability of advanced technical tools for purchase or for free off the Internet.

In the virtual world of cyberspace, malicious cyber activity can instantaneously result in virtual or physical consequences that threaten our economic well being and national security, critical infrastructure, public health and welfare, privacy, civil rights and civil liberties, and confidence in government. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure, and at their time of greatest advantage. Securing cyberspace is similar to protecting physical borders and ports, enforcing and facilitating the immigration laws, securing the aviation and surface transportation system, and preparing to respond from both natural and manmade events: it requires a defense-in-depth approach. Indeed, securing cyberspace is also critical to accomplishing the physical security missions of protecting borders and ports, enforcing immigration laws, aviation security, and responding to natural and manmade events successfully because of the mutual dependence and interconnected nature of the cyber and physical security missions and efforts.

In cyberspace, just as in physical domains, we need to ensure that Federal systems are secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from causing harm. Further, we must use our knowledge of these systems and their interdependencies to prepare to respond should our protective efforts fail. This is a serious challenge, and DHS has made great progress over the past year to improve the nation's overall operational posture and forward-looking policy efforts.

Overview of DHS Cybersecurity Responsibilities

DHS is responsible for helping federal executive branch civilian departments and agencies to secure their unclassified networks, often called the dot-gov domain. DHS also works closely with partners across government and in industry assisting them with the protection of private sector critical infrastructure networks. The Department has a number of foundational and forward-looking efforts under way, many of which stem from the Comprehensive National Cybersecurity Initiative (CNCI).

The CNCI comprises a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- Establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- Defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- Strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the federal government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

DHS plays a key role in many of the activities supporting these goals and works closely with our federal partners to secure our critical information infrastructure in a number of ways. We are reducing and consolidating the number of external connections federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to those TICs. Through the United States Computer Emergency Readiness Team (US-CERT), we are working more closely than ever with our partners in the private sector and across the federal government to share what we learn from our EINSTEIN deployments and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. In addition, the Department has a role in the Federal Government for cybersecurity research and development (R&D). The DHS Science and Technology (S&T) Directorate's Cyber Security R&D (CSRD) program funds activities addressing core vulnerabilities in the Internet, finding and eliminating malicious software in operational networks and hosts, and detecting and defending against large scale attacks and emerging threats on our country's critical infrastructures. The CSRD program includes the full R&D lifecycle -- research, development, testing, evaluation, and transition -- to produce unclassified solutions that can be implemented in both the public and private sectors. The S&T Directorate has established a nationally recognized cyber security R&D portfolio addressing many of today's most pressing cybersecurity challenges. The CSRD program has funded research that today is realized in more than 18 open-source and commercial products that provide capabilities, including the following: secure thumb drives, root kit detection, worm and distributed denial of service detection, defenses against phishing, network vulnerability assessment, software analysis, and security for process control systems.

President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader national cybersecurity strategy. These CNCI initiatives and its associated activities will play the central role in implementing many of the key recommendations of President Obama's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.

With the publication of the *Cyberspace Policy Review* on May 29, 2009, DHS and its components have developed a long-range vision of cybersecurity for the Department's—and the nation's—homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions, as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: to help create a safe, secure, and resilient cyber environment, and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano has consolidated the Department's cybersecurity efforts under the coordination of the National Protection and Programs Directorate (NPPD) and in my role as the Director of the National Cyber Security Center. We are moving aggressively to build a world-class cybersecurity team, and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats. Most immediately, we are focusing on three priorities:

1. Continue enhancement of the EINSTEIN system's capabilities as a critical tool in protecting our federal executive branch civilian departments and agencies.
2. Develop the National Cyber Incident Response Plan (NCIRP) in full collaboration with the private sector and other key stakeholders. The NCIRP will ensure that all national cybersecurity partners understand their roles in cyber incident response and are prepared to participate in a coordinated and managed process. The NCIRP will be tested this fall during the Cyber Storm III National Cyber Exercise.
3. Increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

DHS also bears primary responsibility for raising public awareness about threats to our nation's cyber systems and networks. Every October DHS in coordination with other federal agencies, governments and private industry, make a concerted effort to educate and inform the public through the National Cybersecurity Awareness Month (NCSAM) campaign, and we are making progress. For example, in 2009, the Secretary of Homeland Security and the Deputy Secretary of Defense jointly opened the campaign, we engaged in our most significant outreach ever, and all 50 states, the District of Columbia, and the U.S. Territory of American Samoa, as well as seven tribal governments, endorsed NCSAM.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency or even solely within the Federal realm; it requires teamwork and coordination across all sectors because it touches every aspect of our lives. Together, we can leverage resources, personnel, and skill sets that are needed to accomplish the cybersecurity mission. The fiscal year (FY) 2011 NPPD budget request for cybersecurity strengthens the ongoing work in each of the Department's offices to fulfill our unified mission.

The Office of Cybersecurity and Communications (CS&C), a component of NPPD, is focused on reducing risk to the nation's communications and IT infrastructures and the sectors that depend upon them, and enabling timely response and recovery of these infrastructures under all circumstances. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C is comprised of three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

NCSD collaborates with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructure. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' responsibilities under the CNCI.

Within NCSD, US-CERT leverages technical competencies in federal network operations and threat analysis centers to develop knowledge and knowledge-management practices. NCSD provides a single, accountable focal point to support federal stakeholders as they make key operational and implementation decisions to secure the federal executive branch civilian networks. It is through NCSD's programs that the Trusted Internet Connections Initiative and the National Cybersecurity and Protection System, which I will discuss later, are implemented and upon which stakeholders look to for support during steady-state and crisis. NCSD takes a holistic approach enabling federal stakeholders to address cybersecurity challenges in a manner that maximizes value while minimizing risks associated with technology and security investments. Further, NCSD through US-CERT analyzes threats and vulnerabilities, disseminates cyber threat warning information, and coordinates with partners and customers to achieve shared situational awareness related to the nation's cyber infrastructure.

As I mentioned before, the Department is responsible for supporting federal executive branch civilian agencies in the protection and defense of their networks and systems. The Department's strategy, which supports a defense-in-depth, requires situational awareness of the state of federal networks, an early warning capability, near real-time and automatic identification of malicious activity, and the ability to disable intrusions before harm is done. DHS, through NCSD and US-CERT, developed a "system-of-systems" approach to support its cybersecurity mission (noted above). This overall system-of-systems is known as the National Cybersecurity Protection System (NCPS). As part of the NCPS, DHS is deploying a customized intrusion detection system, known as EINSTEIN 2, to federal executive branch civilian agencies to assist them in protecting their computers, networks, and information.

None of this is possible, however, without a comprehensive understanding of federal executive branch civilian networks from an enterprise perspective. The CNCI TIC initiative provides the federal government this understanding by reducing and consolidating external access points across the federal enterprise, assisting with the security requirements for federal agency network and security operations centers, and establishing a compliance program to monitor federal agency adherence to TIC policies.

The Department is installing EINSTEIN 2 capabilities on federal executive branch civilian networks in distinct but interconnected steps. The first step, under the TIC initiative, is the consolidation of external connections and application of appropriate protections thereto. This will help create an efficient and manageable front line of defense for federal executive branch civilian networks. The goal is to get down to less than 100 physical locations. Our program office has been working with departments and agencies to better understand how civilian agencies configure their external connections, including Internet access points, and improve security for those connections. As departments and agencies are consolidating their external connections, we are working to deploy EINSTEIN 2 to these TIC locations to monitor incoming and outgoing traffic for malicious activity directed toward the federal executive branch's civilian unclassified computer networks and systems. EINSTEIN 2 uses passive sensors to identify when unauthorized users attempt to gain access to those networks. EINSTEIN 2 is currently deployed and operational at 11 of 19 departments and agencies. The EINSTEIN 2 system is already providing us with, on average, visibility into more than 278,000 indicators of potentially malicious activity per month.

The TIC initiative and EINSTEIN 2 deployments are critical pieces of the federal government's defense-in-depth cybersecurity strategy. DHS is also building upon the enhanced situational awareness that EINSTEIN 2 provides. We currently are working with the private sector, the National Security Agency, and a wide range of other federal partners to test the technology for the third phase of EINSTEIN, an intrusion-prevention system which will provide DHS with the capability to automatically detect malicious activity and disable attempted intrusions before harm is done to our critical networks and systems.

For all these deployments, it is important to note that EINSTEIN capabilities are being carefully designed in close consultation with civil liberties and privacy experts—protecting civil liberties and privacy remains fundamental to all of our efforts.

These accomplishments are reliant upon increasing the number of dedicated and skilled people at CS&C. To this end, the National Cyber Security Division tripled its federal workforce from 35 to 118 in FY 2009, and we hope to more than double that number to 260 in FY 2010. We are moving aggressively to build a world-class cybersecurity team, and we are focusing on key priorities that address people, processes, and technology.

Recently, the Office of Management and Budget (OMB) and the President's Cybersecurity Coordinator issued new Federal Information Security Management Act (FISMA) reporting requirements that will help our cybersecurity workforce to inculcate a culture of cyber safety. The new requirements are designed to shift efforts away from compliance on paper and towards implementing solutions that actually improve cybersecurity. The new reporting requirements will automate security-related activities and incorporate tools that correlate and analyze information, giving the government's cyber leaders manageable and actionable information that will enable timely decision-making. DHS will provide additional operational support to agencies in securing their networks by monitoring and reporting agency progress to ensure the new OMB/ Cybersecurity Office guidance is effectively implemented. This new reporting follows a three-tiered approach:

- Data feeds directly from security management tools—agencies are already required to report most of this information. It includes summary information on areas such as inventory, systems and services, hardware, software, and external connections.
- Government-wide benchmarking on security posture—which will help to determine the adequacy and effectiveness of information security, civil rights and civil liberties, and privacy policies, procedures, and practices throughout the government.
- Agency-specific interviews—which will be focused on specific threats each agency faces and will inform the official FISMA report to Congress.

Response to Legislation

DHS welcomes working with the Committee on strengthening the Department's ability to accomplish its cybersecurity mission—securing federal executive branch civilian systems and working with the private sector and federal sector-specific agencies to secure the nation's CIKR.

- We appreciate support for DHS' mission in implementing cybersecurity for federal civilian networks, working in partnership with the private sector to secure critical infrastructure systems and functions.
- The Department is looking to maximize its hiring flexibilities in support of fulfilling its cyber mission.
- The Administration currently is reviewing the appropriate scope of authority to ensure that the Department's cybersecurity mission can be achieved, and we look forward to continuing to work with Congress in this regard. Regulatory agencies in sectors such as banking, finance, energy, transportation, healthcare, and communications should continue to review existing cybersecurity regulatory requirements and determine if new rulemaking is required. These sectors should continue to consult with DHS and the National Institute for Standards and Technology during this process.
- The bill recognizes that Americans expect the federal government to anticipate, prevent, and respond to cyber threats. The provisions relating to imminent cyber threats acknowledge that the government may need to take extraordinary measures to fulfill these responsibilities.

Section 706 of the Communications Act and other laws already address Presidential emergency authorities and Congress and the Administration should work together to identify any needed adjustments to the Act, as opposed to developing overlapping legislation. We will continue to assess this issue and others that touch on the relationship between government and the private sector.

- DHS also welcomes the fact that this legislation ensures that privacy and civil liberties protections will continue to be fully integrated into our cybersecurity operations.
- With regard to the revised FISMA provisions, the Administration has begun significant FISMA reform that streamlines and updates the process and increases the focus on outcomes. The Administration is developing new policy guidance to clarify the role of DHS in Federal cybersecurity activities.
- While this Committee and DHS clearly share the common goal of increasing the Department's capabilities to meet the cybersecurity mission, we believe that it is preferable to maintain a singular organizational integration between physical and cybersecurity operations, rather than create a separate cyber organization.
  - This Committee is well aware of Supervisory Control and Data Acquisition (SCADA) systems—the electronic systems that allow infrastructure owners to remotely operate our dams, our power generation plants, and our transportation networks. The NPPD Office of Infrastructure Protection empowers private and public stakeholders to protect these assets through vulnerability assessments and an active field presence. CS&C, moreover, monitors cyber-based threats and vulnerabilities that could compromise SCADA systems and also engages directly with asset owners to mitigate risk. These physical infrastructure and cybersecurity efforts are best enabled by maintaining and expanding organization connection, thus promoting efficiencies, providing expanded situational awareness, and helping to keep America running.
  - We continue to believe that the nexus point between critical (physical) infrastructure that have cybersecurity vulnerabilities, such as the electrical grid which could potentially be hacked through the Internet, can best be made resilient through a single organizational entity that works to prevent, mitigate, and recover from all-hazards attacks where the lines of cyber and physical security are erased.

Conclusion

Mr. Chairman, Ranking Member Collins, Members of the Committee, thank you again for your strong support of the Department, and for your dedication to improving cybersecurity. We look forward to working with you to strengthen efforts that are critical to the nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the nation and keep Americans safe.

Thank you for again for this opportunity to testify. I would be happy to answer any of your questions.

Senate Homeland Security and Government Affairs Committee

Protecting Cyberspace as a National Asset:
Comprehensive Legislation for the 21st Century

Statement for the Record

Frances Fragos Townsend
Chairwoman of the Board
Intelligence and National Security Alliance

June 15, 2010

Chairman Lieberman, Ranking Member Collins, Senator Carper and members of the Committee, thank you for the invitation to testify at this hearing and to offer my thoughts on the *Protecting Cyberspace as a National Asset Act of 2010.* I am here today in my role as the Chairwoman of the Board of the Intelligence and National Security Alliance (INSA). INSA is the premier not-for-profit private sector professional organization providing a structure and interactive forum for thought leadership, the sharing of ideas, and networking within the intelligence and national security communities. INSA has over 100 corporate members, as well as several hundred individual members who are leaders within the government, private sector and academia.

Through its Cyber Security Council, INSA has emphasized the importance of creating a strong public-private partnership that can provide meaningful recommendations to address this national and economic security threat. Today I would like to specifically speak to the importance of establishing a public-private partnership to promote national cyber security priorities, strengthen and clarify authorities regarding the protection of federal civilian systems, and improve national cyber security defenses.

Collective national cyber security can only be effectively addressed through a partnership approach between government and private industry. While the government has the legal and moral authority required to organize markets, enforce laws and protect citizens' privacy and property, the vast majority of cyberspace infrastructure is privately owned and operated. As a result, industry is where most of the expertise in the fields of IT and cyber security reside. The private sector cannot protect privacy and address security while the government cannot dictate security regulations to networks systems it cannot control. Furthermore, attempts to do so could stifle innovation and profitability. Because of this dynamic, partnership is the only way forward.

INSA's Cyber Security Council studied several different models of public-private partnerships during the preparation and research for its November 2009 report, *Addressing Cyber Security Through Public-Private Partnership.* Historically, effective public-private partnerships have inclusive private sector membership, unified in the pursuit of common goals, a single responsible and accountable government partner organization and clearly delineated roles for both public and private entities. We are very pleased to see these concerns and this organizational structure reflected in the legislation we are discussing today. This bill not only establishes a clearly responsible Center for the problem, but requires that a private sector advisory council be organized to advise the Center on their actions' effects on industry.

Assuring that private sector concerns are heard within government is an important first step to the creation of a public-private partnership, but this alone is not sufficient to guarantee success. INSA's Cyber Security Council has identified three key additional components, specific to a public-private partnership on cyber security, which would be required for a successful effort: a flexible or incentivized approach to regulation, robust information sharing and cooperation and communication on standards and best practices.

With regards to flexible and/or incentivized regulation, it is crucial that government, to the best of its ability, preserve and nurture the innovative and entrepreneurial environment that exists in information technology. A free flow of information and the use of an open source environment has created capabilities and driven the development of new business. Prescriptive or directive security standards, or one-size fits all approaches will limit innovation and erode industry support and participation if industry managers feel security mandates have made their business less competitive. Securing networks and the cyber environment while allowing businesses to remain dynamic in that space is a difficult needle to thread and we applaud the measured approach of this bill in allowing industry members to propose their own security solutions for approval by the regulatory body. This not only creates a true give-and-take security partnership, but also allows for innovation and growth with the development of new procedures and products.

Also critical to a strong public-private partnership is the creation of a shared awareness of the network environment. Information sharing is absolutely crucial and is an area in which we are presently falling short. Classification, concerns over liability and the present situation in which cyber security is not "owned" by anyone all contribute to this shortcoming and there are sections of this bill that do help. The liability protections afforded to those in compliance with government security measures do provide protection and incentive to private sector firms to increase their reporting, but until the private sector feels they are getting as much as they are giving with respect to information sharing and incident reporting, the system will remain insufficient. The bill calls for the establishment of plans for information sharing between public and private entities and industry should certainly watch this process closely and press for a commitment from the executive branch to share information with the private sector that is as strong as the private sector's responsibility to report to the government.

The final component, cooperation in the development of standards and best practices, is perhaps the most crucial. Government must develop security standards and systems that deal with known threats and have the capacity to adapt to the rapidly changing cyber environment, and it must do so in concert with industry partners. Just as directive regulations can limit innovation, security standards that are not developed in partnership with businesses can have adverse and unplanned consequences. The vetting of proposed security standards through the industry community is necessary to avoid undue burden and hardship for American business. But the private sector cannot carry out this process entirely on its own; they need strategic-level threat information and cross-sectional situational awareness from the government to create standards which address actual threats and vulnerabilities and make the nation safer. In this bill, the new Center for Cyber security and Communications assesses and evaluates cyber security standards and guidelines, and makes recommendations recognizing existing NIST and industry standards, an important step toward joint production of security protocols. The second step must be carried out by the Center itself when creating its standards and bringing them to industry. They should embrace a true partnership approach, soliciting comments from industry on draft proposals, consulting closely with owners and operators and being open to revision of their rules in light of industry input.

The INSA Cyber Security Council recognizes that there are a number of ways to address cyber security and believes the effort to do so should begin right away on three fronts: private sector self-regulation, executive branch leadership and congressional action. Self regulation is not an unprecedented activity in the U.S private sector. There are multiple examples of where the private sector has self-organized to attain a goal. Examples are the North America Electric Reliability Corporation, volunteer Fire Departments, school boards, community associations, etc. Self regulation in cyber space can be achieved and self imposed based on a strong value proposition and value-based incentives. However, only the government, contained by law, can fully investigate the behavior of individuals or groups, apprehend, prosecute and punish those who violate the law or defend against and respond to threats and attacks against the nation's interests. Hence a government role, within DHS like the one identified in the bill, is absolutely essential.

Finally, the role of Congress to enhance the security and resiliency of the cyber and communications infrastructure of the United States is critical to make well-informed decisions and respond to problems quickly. Congressional oversight is also important to ensure that the goals and objectives of the National Strategy are being met, particularly as they relate to use of legal authorities for cyber missions and the reasonable privacy expectations of U.S. persons.

With this bill, the Senate has taken the lead in identifying cyber security needs and organizing the government to address them. This measure relies on the executive branch for the establishment, implementation and development of new structures, protocols, plans and oversight. This Committee, as well as the private sector will have to engage with the executive branch and monitor the implementation of the provisions of this bill to ensure that this new organizational structure reflects the spirit of the law and does not place undue or unanticipated counterproductive burdens on both government agencies and private sector companies. The goal is to make a positive and meaningful contribution to the national security of the United States and this bill goes a long way towards achieving that goal.

Testimony of Alan Paller

Director of Research, The SANS Institute

Before the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Hearing on

"Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century"

June 15, 2010

Chairman Lieberman, Ranking Member Collins, Senator Carper and Members of the Committee, you made last Thursday a very good day for improving the security of our nation. On that day, you introduced Senate Bill S 3480, and began the process of transforming federal information security so that the government can lead by example in making America's computers and networks much safer than they are today.

In support of that goal, my written testimony has two sections: one shows how much trouble the nation is in and exactly how the legislation you present enables the nation to correct the errors that got us into that trouble in the first place, and (2) what effective cyber security means, including how innovative federal employees and organizations are demonstrating that effective security can be implemented in government. This second part includes some small adjustments in S 3480 that would enable it to be more effective in transforming cyber security. The testimony also illuminates the misleading arguments put forth by interest groups determined to delay the critical improvements that your legislation enables, because it suits their own economic interests.

Part 1: How Much Trouble is the U.S. In? And Why?

Our country is by far more dependent on the Internet than its adversaries.; several of whom may be able to disconnect their systems from the Internet for a time and still operate; we cannot. That means our cyber defense must be near perfect. It is not even close. The systems that most Americans and American enterprises purchase and deploy on the Internet are full of programming errors that adversaries exploit to gain access and install remote control tools, or what General Alexander, Commander of the US Cyber Command, calls "remote sabotage tools."

According to the Commander of the Navy's 10th (Cyber) Fleet, Adm. McCullough, flaws and remote control tools could very well compromise our control over kinetic weapons. The US has a major advantage over its adversaries in that it can destroy enemy assets using missiles, bombs, planes, ships, artillery, and bullets. But that lead, says Adm. McCullough, disappears "if I don't own my command and control computers." While adversaries invest more in cyber weapons and cyber talent, the US keeps increasing our investment in kinetic weapons, and paying lip service to the cyber skills that will keep them within our control. "We are on the wrong side of the cost curve," Admiral McCullough added.

Seven weeks ago, the Deputy Assistant Director of the FBI for Cyber provided a bracing description of the nation's cyber risk. The cyber threat "can challenge our country's very existence," said Steve Chabinsky. "How we rise to the cybersecurity challenge will determine whether our nation's best days are ahead of us or behind us." Vice Admiral Mike McConnell, Director of National Intelligence under President George W. Bush, had already put a fine point on the problem, telling the Senate Commerce Committee on February 23, 2010, "If we went to war today in a cyberwar, we would lose."

This is not just a problem in our military systems. The critical infrastructure on which we are so reliant and, indeed, the intellectual products that are critical to our place in world markets are in jeopardy. Computer systems supporting electric power generation and distribution are already infested with those remote control infections described by General Alexander, as are computers in federal and state government agencies.

The US is also losing its most sensitive intellectual property – the foundation of our nation's economic and strategic advantages. A Commerce Department official testified to a House of Representatives panel in the aftermath of a cyber attack where the Chinese stole extensive technical data on all US technologies too sensitive to be exported. The official said that he and his experts had no idea how far the infections had spread through the Agency's computers nor whether the infections had been found and removed.

Cyber attackers also penetrated the defense industrial base multiple times over several years. In one case, the target was a major defense contractor's computers, where sophisticated attackers made off with electronics and design data on advanced weapons that were to be deployed on the Joint Strike Fighter, America's most expensive weapons system costing American taxpayers around $300 billion. According to the Wall Street Journal, "Six current and former [federal] officials familiar with the matter confirmed that the fighter program had been repeatedly broken into." The defense industrial base is the most valuable and fertile target for nations that want to steal military technology data rather than fund their own technology research.

Additionally, an epidemic of intellectual property cyber theft is plaguing companies and their law firms and their consultants, especially those doing business with Asian nations. You heard in January about the successful attacks on Google, Intel, Adobe, and Yahoo, resulting in the loss of extremely valuable intellectual property. They are not alone. Although US companies never were told of the scale of the threat, and who was at risk, British companies were. The head of MI-5 (the UK Security Service) sent a letter to the managing directors of the 300 largest companies in the United Kingdom in late 2008. The letter said that if they are engaged in any negotiations or business with a major Asian power, they are being attacked with the same cyber weapons that are used against military targets. The attackers' goal is economic advantage - to give their own countries' companies a leg up in negotiations or even eliminate the need to negotiate at all since they can get the valuable intellectual property through cyber exploits. That letter also told the British companies that their law firms were being targeted. Many hundreds of US companies have had their systems penetrated and their data stolen and remote control software installed. Some of the largest US law firms have been deeply penetrated with their entire databases of all client records having been stolen.

US government sites have been infected and used in criminal activities. Computers at the Department of Transportation delivered pornography for several weeks. News articles reported a web site at the Department of Homeland Security was sending Trojan horse software to web visitors' computers in an attempt to take over those computers and use them in financial cyber crimes. While some of these crimes are for financial gain and some just for what seems to be mischief, they demonstrate the extent of our vulnerability.

Cyber crime is also lucrative for terrorists - to get money to buy the bombs to kill innocents. Imam Samudra, the Bali Bomber, who exploded a bomb and murdered 200 young vacationers from Australia and New Zealand in October 2002, used cyber crime to get money to buy bomb-making supplies. He wrote his autobiography while on death row. In it, he gave Al Qaeda recruits detailed instructions for using cyber crime to "make more money in a few hours of work than a policeman can make in three to six months of work." He went on to say, "Please do not do that in the sake of money alone! I want America and its cronies to be crushed in all aspects."

How Did the Nation Become So Vulnerable?

The government and critical infrastructure organizations are terribly vulnerable because, in their successful quest for automation, they unknowingly purchase and deploy computer software and hardware that have design flaws and software bugs. Those vulnerabilities enable cyber spying and cyber crime, most of which could have been avoided. But, instead of working cooperatively with the IT industry to limit the risk and minimize the damage, agencies spend billions of dollars paying consultants to write reports that are out-of-date before they are printed and that

Additionally, an epidemic of intellectual property cyber theft is plaguing companies and their law firms and their consultants, especially those doing business with Asian nations. You heard in January about the successful attacks on Google, Intel, Adobe, and Yahoo, resulting in the loss of extremely valuable intellectual property. They are not alone. Although US companies never were told of the scale of the threat, and who was at risk, British companies were. The head of MI-5 (the UK Security Service) sent a letter to the managing directors of the 300 largest companies in the United Kingdom in late 2008. The letter said that if they are engaged in any negotiations or business with a major Asian power, they are being attacked with the same cyber weapons that are used against military targets. The attackers' goal is economic advantage - to give their own countries' companies a leg up in negotiations or even eliminate the need to negotiate at all since they can get the valuable intellectual property through cyber exploits. That letter also told the British companies that their law firms were being targeted. Many hundreds of US companies have had their systems penetrated and their data stolen and remote control software installed. Some of the largest US law firms have been deeply penetrated with their entire databases of all client records having been stolen.

US government sites have been infected and used in criminal activities. Computers at the Department of Transportation delivered pornography for several weeks. News articles reported a web site at the Department of Homeland Security was sending Trojan horse software to web visitors' computers in an attempt to take over those computers and use them in financial cyber crimes. While some of these crimes are for financial gain and some just for what seems to be mischief, they demonstrate the extent of our vulnerability.

Cyber crime is also lucrative for terrorists - to get money to buy the bombs to kill innocents. Imam Samudra, the Bali Bomber, who exploded a bomb and murdered 200 young vacationers from Australia and New Zealand in October 2002, used cyber crime to get money to buy bomb-making supplies. He wrote his autobiography while on death row. In it, he gave Al Qaeda recruits detailed instructions for using cyber crime to "make more money in a few hours of work than a policeman can make in three to six months of work." He went on to say, "Please do not do that in the sake of money alone! I want America and its cronies to be crushed in all aspects."

How Did the Nation Become So Vulnerable?

The government and critical infrastructure organizations are terribly vulnerable because, in their successful quest for automation, they unknowingly purchase and deploy computer software and hardware that have design flaws and software bugs. Those vulnerabilities enable cyber spying and cyber crime, most of which could have been avoided. But, instead of working cooperatively with the IT industry to limit the risk and minimize the damage, agencies spend billions of dollars paying consultants to write reports that are out-of-date before they are printed and that have no substantial effect on reducing the security vulnerabilities. To demonstrate how important Senate oversight can be, this multi-billion dollar waste was uncovered by Senator Carper and his staff and illuminated in a Senate hearing last fall. His work has already moved the White House to begin reshaping federal cybersecurity, but your bill is still needed to empower and accelerate that change.

The continuing financial waste that Senator Carper uncovered amounts to about $400 million each year. That's enough, when combined with innovative use of federal IT procurement, to fund government-wide implementation of near-real-time situational awareness. In other words, if the bill you are considering is passed, and if you continue the kind of oversight Senator Carper demonstrated, the agencies will have enough savings from avoiding manual reporting to pay for the automation needed to significantly reduce their cyber risk.

Did the Old FISMA Actually Cause the Problem?

Here's the evidence. It begins with one of the contractors explaining why his company produces the "useless" reports and then tracks the authorities all the way back to FISMA.

(1) Mike Jacobs served as Information Assurance Director at NSA. When he retired from the NSA, he took a management role at a government contractor where he oversaw the work of 200 consultants who produced FISMA reports. He told a group of retired federal officials and his own staff, "You know, the only reason we write those stupid reports is that our government customers demand them."

(2) Government CISOs are the "government customers" who hire the contractors to write the FISMA reports. The CISOs told me repeatedly the reason they spend the money to produce the reports is that OMB demands that they do them. If they don't produce the reports, their Departmental deputy secretary will get chewed out by the OMB folks, and he'll come back and task the CIO and CISO with doing them. The pressure to pay for expensive reports causes real problems for the CISO. A CISO in one large agency told a reporter in 2004 that FISMA reporting was already consuming such a large part of her budget that she did not have the funds needed to build stronger defenses. Other CISOs repeat that statement in private.

(3) But why don't the CISOs fix the problem by focusing their limited funds on the most critical controls that can actually reduce risk rather than produce voluminous reports covering lots of old, less critical information? "Because," the CISOs say repeatedly, "FISMA states that NIST standards and guidance are mandatory. " That empowers the Inspectors General and OMB staff to demand CISOs do everything in the NIST guidance. When you demand that someone perform huge numbers of things, with limited budgets, you get dysfunctional results. One illuminating example is the department in which a

> full grade was lost on the annual FISMA scoring because the departmental IG demanded that every employee be given security awareness training. A full letter grade was lost because the department hadn't trained all the people who do the gardening and landscaping; meanwhile the IG never checked to see whether all systems were configured securely.

One last question for the dialogue: Since FISMA assigned NIST the unlimited power to set the standards, why did NIST not develop standards that enabled cost-effective vulnerability and risk reduction? The answer is that there are wonderful people at NIST, with great intentions, but most have never secured a computer (at least in the past decade), cleaned up after an attack, performed deep packet analysis or reverse engineering or memory forensics. In other words they don't know how the attacks work so they cannot know how to prioritize their guidance. How could a doctor prioritize treatment for patients if he or she had no experience with what works and what doesn't work? Perhaps even worse, NIST contracts out much of the guidance drafting. The very same companies hired to write the guidance then turn around and charge agencies tens or hundreds of thousands of dollars for reports that comply with NIST guidance, but are out-of-date and not useful.

Does Senate Bill S 3480 Fix the Other Problems With FISMA?

The legislation undoes the central error of FISMA by removing the requirement that FISMA guidance documents are mandatory. Ed Roback, now CISO at Treasury but who led the NIST team that developed most of the guidance documents, stated repeatedly that making NIST guidance mandatory was wrong.

Senate Bill S 3480 also presses agencies to stop spending money on out-of-date reports and instead focus their spending on continuous monitoring and risk reduction. It provides a Senate-confirmed cyber coordinator in the White House with the power to ensure NIST's documents do not mislead agencies into spending money on the wrong defenses. I hope that the White House office can also help focus inspectors general and GAO auditors on the important elements of NIST guidance so those auditors become part of the solution. That same White House office will also help OMB make certain that federal IT procurement ($80 billion per year) is used as an effective incentive for vendors to deliver software and hardware that has far fewer security holes and that is much easier to maintain securely than is currently being delivered.

Sadly, there are highly paid antibodies at work in Washington, who wrongly see their employers' wealth increasing if the implementation of S 3480 is delayed. That means that the critical changes envisioned by your bill won't happen unless you maintain vigorous oversight through the transition to dynamic, automated security. I'm not worried. You have phenomenal staff, on both sides of the aisle, as do several other committees. If your committee continues to work with the other committees on active oversight, I think you will be extremely proud of what you accomplish in making the nation a much tougher target for cyber attacks.

Other Remarkable Aspects Of S 3480

Four other aspects of S 3480 deserve recognition.

First your procurement and supply chain language is both important and innovative. It is important because the principal vector for positive control of an adversary's computers is to embed code while the technology is being manufactured. Finding hidden code is challenging and will require enormous resources. The issue really needed the language in your bill to raise its priority. It is missing one requirement: testing. You can't find flaws if you don't look for them and you find them by having the suppliers use a suite of automated testing tools that verify everything that can be tested is free of flaws – whether the flaws were accidental or intentional.

The language is also innovative because it avoids the mistake of requiring supply chain language in the Federal Acquisition Regulations (FAR) and instead requires that language to be made part of the actual contract specifications. The FAR demands more than any contractor can do; so, in nearly every case, contractors do what is in the actual contract specifications and hope no one calls them on FAR compliance. It's a strategy that has worked well for at least three decades.

Second, kudos to the drafters because this may be the only bill I have ever seen where a later draft requires fewer reports from the executive branch than earlier drafts. Reports chew up enormous amounts of time of the best people in government, taking them away from the tasks you really want them to accomplish. You have demonstrated a willingness to ask for reports only when you know what the value will be in having the report prepared. I hope other committees follow your example.

Third, the regulatory framework and the emergency measures you establish for the critical infrastructure is long overdue. Without it, there will be no defense of the critical infrastructure in place when a major cyber attack is launched against the United States. One caveat. The structure might not be as effective as it needs to be. Some of the language will lead to long delays in implementing effective defenses. Long delays do not help the nation, they help the vendors that sell IT products and services to government and want government to accept their products as they are without being asked to make sure those products are secure. The vendor representatives (and their associations) are employed by government affairs and marketing departments of vendors that sell billions of dollars of sometimes flawed technology to the government. Their ample salaries are paid for by corporate officers who usually tell them that they have only two jobs in Washington: (1) to make sure the government does nothing that will cost their company money and (2) that if they can find some extra federal revenue for their employer, that's a bonus. Their most effective tool in accomplishing their mission is delay, with their favorite delaying tactic being language in legislation that forces federal agencies to get IT industry review or consult with industry before acting. Notice that this tactic also gives the industry reps access to inside information that their sales people use to tap into new money the government will spend. If you agree the risk is real, perhaps it's time to stop acceding to their delaying tactics.

Fourth, the Manpower section will help DHS build its cyber employee base and help grow the workforce, but it needs one critical change. It calls for training of people with specialized security skills, but has no mechanism to assure the training was effective; that the trainer even knew how to do the job for which the trainees were being prepared and that the trainees came out of the training process with actual hands-on specialized skills to do the job. For too long people could read a book, pass a test and call them selves certified information security professions. Accepting unskilled people for important roles was a major cause of the nation becoming so vulnerable. If you add a requirement to validate the skills of each contractor employee and to prove those skills are the ones needed for each specialized job, you'll have a big impact. Without that, the Manpower section will lead to lots more people employed in cyber security, but without the necessary specialized skills. The best approach is to use procurement language. When the contractors can win new projects only with highly skilled people; they will act quickly to develop the skills the nation needs.

Part 2: Effective Cyber Defense; the Federal Initiatives that Show How It Can Work; and the Ways Private Economic Interests Attempt To Block It

Dynamic Defense

Dynamic defense automates cyber risk reduction and eliminates the manual processes that allowed our nation's networks and systems to become so vulnerable to cyber attack. Our adversaries are far too agile for us to rely heavily, as we have until now, on periodic human evaluations of the state of our systems and networks and human interventions after the fact. A far more effective approach to cyber security is called "dynamic defense." That's what Admiral McCullough, Commander of the 10th (Cyber) Fleet promised the Chief of Naval Operations he would deliver this year.

It has two parts as described by Admiral McCullough:

(1) Near-real-time situational awareness so we can see what is going on in the network just like we monitor an air warfare battlespace.

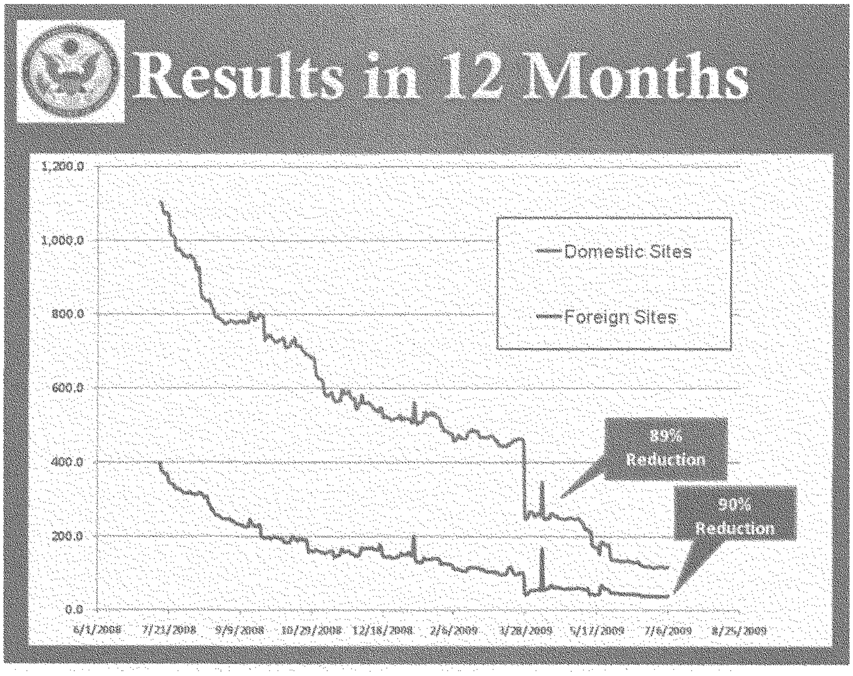
(2) Once we achieve near-real-time situational awareness, then we need to dynamically defend the network in near-real-time.

What he is describing is not a theoretical construct. We know that it can work. The U.S. Department of State Department proved that near-real-time situational awareness is both possible and powerful. At the State Department, they call it continuous monitoring.

The State Department Proves Continuous Monitoring Works

Two of the most important benefits of dynamic defense are enabling the defenders to (1) minimize their vulnerability to attack, and (2) act very quickly to protect their systems when a new threat or vulnerability is discovered. Continuous monitoring, the first step in dynamic defense, enables both of those goals to be met much more effectively than FISMA-based quarterly or annual reporting. Strong support of continuous monitoring, in lieu of out-of-date report writing, is one of the most important elements you have included in Senate Bill S 3480. The State Department is the only agency that has implemented continuous monitoring so far, although there are credible rumors that the Army, NASA and NSA are moving that way. And the Navy doesn't seem to be far behind and the Air Force is leaning in the right direction.

Continuous monitoring works. Figure 1 shows that the U.S. State Department was able to reduce reliably-measured risk by over 85% in less than a year. State is continuing the process with equally impressive results this year. Look closely at the chart, and you will see what continuous monitoring means – the updated data comes in daily or every couple of days – not quarterly, or annually. Had State used the longer time periods favored by the other agencies, many more State Department computers and networks would have been open to attack, for far longer periods,



Results in 12 Months

Continuous monitoring also radically reduces the time it takes agencies to fix important new security problems. Here's proof: When Google announced it had been penetrated and had lost sensitive data, it simultaneously illuminated a major vulnerability, nicknamed Aurora. Aurora was present on millions of machines across the government (those running Internet Explorer). Fixing Aurora turned into a positive case study of the effectiveness of State's continuous monitoring initiative.

Federal agency CISOs all learned from news reports or from US-CERT at DHS that most of their computers were at high risk of compromise from attacks using the Aurora vulnerability. Each CISO acted quickly, using the tools available. Nearly all of them sent out email notices to their distributed security officers who sent out email notices to system administrators. Sadly, many of those system administrators did not act. There was no centralized monitoring of patch status, so the civilian agency CISOs had no way of even knowing. If what gets watched gets done, then the CISOs' lack of near-real-time visibility into their networks makes them unable to protect the computers for which they are responsible. DoD, on the other hand, demands that the recipients of the security patch orders (called IAVAs) confirm receipt and confirm whether the correction has been implemented. A DoD official told me the confirmation reports showed that fewer than 70% of the vulnerable machines were patched even five months after the mandatory Aurora order went out.

The State Department offers a stark contrast to DoD and other agencies, because State can tell, within a day, which systems have and have not been patched. When State's CISO learned of the critical problem posed by the Aurora vulnerability, he didn't have to send an email. He raised the vulnerability's risk factor (the value used to weight it in the overall risk score). Every office saw immediately that their security score had fallen and their bosses also saw the fall. Within 6 days 90% of all vulnerable systems in all embassies and in all State Department offices around the world had been patched and were safe from attacks. That's six days, not weeks or months. No emails had to be sent; the scoring risk system did all the work. A clear example of why daily continuous monitoring is so important: it causes rapid risk reduction with low overhead.

Every federal agency can have the same results or better. They already have the vast majority of tools they need to automate continuous monitoring of the most critical controls defined by NSA, DHS, DoD, and the DoE nuclear energy labs. Those are the same controls measured by the State Department to be certain they are doing the most important things first. And the State Department's CISO, John Streufert, generously provides copies of State's management and scoring software at no cost to other U.S. government and defense industrial base organizations.

You might assume from this discussion that the original FISMA enables such automation. The exact opposite is true. The CISOs tell me that they cannot follow in State's footsteps because their money is tied up paying for those out-of-date reports. As mentioned earlier, those reports are required, according to the CISOs, because FISMA made NIST guidance mandatory. What your bill calls for in continuous monitoring is a new way of managing federal security, one that has already proven it is far more effective than the old way.

How Private Economic Interests Fight Continuous Monitoring

Sadly, it is not only FISMA that is slowing down the move to near-real-time situational awareness through continuous monitoring. The contractors that charge federal agencies hundreds of millions of dollars for writing the out-of-date reports are fighting to stop the move to continuous, daily monitoring, even though they and their firms can continue to be employed to enable and manage the new way of doing business. Their rear-guard actions are being supported by federal officials who appear to be uncomfortable with change or afraid of taking responsibility for active risk reduction. Box 1 below summarizes the evidence.

Misleading Statement 1

"We are already doing continuous monitoring."

In a SecureAmericas meeting in Washington late last month, Hord Tipton, the host and ICS2's president, asked the 150 federal security contractors and information security officers in his audience, "How many of you are already doing continuous monitoring?" He told me that more than 130 people raised their hands. Both Hord

> and I know that they didn't mean continuous monitoring the way the State Department is doing it, so I did some research. It turns out that the people who raised their hands are calling manual data entry of quarterly or annual or tri-annual reports "continuous monitoring." This is how the consulting firms can continue to get paid hundreds of thousands of dollars for reporting out-of-date information; they'll enter it into a computer system rather than print it and put it in 3-ring binders.
>
> What they call continuous monitoring is the opposite of what the State Department has done; it does not enable rapid risk reduction or rapid response to new threats. What it does do is give the people who want to continue writing useless reports a cover story. I wondered how so many people could justify the deception and learned that NIST was the source. Both at the NIST website, and in speeches by NIST executives, viewers and attendees are told that NIST's updated Special Publication 800-53 guidance enables continuous monitoring. The only way that could be true is if annual or quarterly manual information collection is renamed "continuous monitoring." Lo and behold, that is just what NIST did. NIST's 800-53 publication is employed by CISOs and contractors to guide and justify the $1,400 per page reports that have almost no impact on risk reduction. In other words, the people who are desperate to keep writing reports stole the term "continuous monitoring" to cover up their continuing antagonism to actually measuring and reducing risk. You can avoid having your new bill hijacked by the paper pushers if you add three words ("data entry and") to your definition of continuous monitoring [3551(b)(2)] and if you use oversight to shine a bright light on counter-productive behaviors.

Despite the delaying tactics describe above, many agencies are trying to follow the State Departments lead, and some, such as the Air Force, are finding other innovations in continuous monitoring.

The 24th Air Force Takes Continuous Monitoring A Step Further

The 24th (Cyber) Air Force has responsibility for securing the entire US Air Force network. A few months ago away teams from the 24th discovered that more than 30% of anti virus (AV) packages across the Air Force were not up to date. No amount of email cajoling was effective. So Colonel Diaz, Operations Director, and General Weber, Commander of the 24th, had their people build automated monitoring tools that continuously check AV updates. Their solution is different from what most other organizations use because it is open and works well with multiple antivirus tools, avoiding the vendor lock-in that is so damaging to innovation and cost-effectiveness. The Air Force system goes beyond testing. Every time it finds a computer with out-of-date anti-virus signatures, it immediately connects that computer to a special network where it gets an AV update. An out-of-date system is not reconnected to the main network until it is protected and cleaned if it has become infected. On General Weber's order, the technology is being deployed across all of the Air Force.

This innovation by the 24th Air Force extends a tradition of Air Force cyber leadership that began in 2002, as I describe in the next section.

Procurement is the Most Productive Public Private Partnership for Improving Federal Cybersecurity – The Air Force Standard Desktop Story

In 2002, US Air Force CIO John Gilligan determined that the Air Force was spending more to test and deploy patches and to clean up after the damage from flaws in Microsoft software than to buy the software, and he announced he was going to ask Microsoft to work with him to solve the problem. He tasked NSA and Air Force experts with determining a safe configuration of Microsoft Windows that would withstand common cyber attacks as well as attacks used by NSA's red teams, and still effectively operate Air Force applications. Once that was done, he negotiated a contract with Microsoft to deliver the secure version of its software to the Air Force, through its hardware suppliers, such as HP and Dell. Microsoft also agreed to test all new security patches on the Air Force secure configuration before the patches were released. More than 550,000 Air Force PCs had the secure desktop installed. Gilligan was succeeded in the Air Force CIO job by Lieutenant General Peterson, who told me that the innovative partnership between Microsoft and the Air Force saved the Air Force over $100 million per year in reduced system administration staff and reduced patch testing. He also said it reduced the average patch installation time from 57 days to 72 hours and is on its way to 24 hours. And he said that the help desk calls had been cut in half because the users were able to get their work done and they were much happier. The bottom line of this procurement partnership: huge savings, huge improvement in security, and huge improvement in user satisfaction. What is not widely known is that the secure configuration purchased by the Air Force also protects Air Force systems from most infections carried by the Advanced Persistent Threat that has plagued so many other federal agencies.

The Air Force secure Windows procurement cost about $100 million per year, and that was money they had to spend anyway for Windows updates. But by consolidating all Air Force procurement into a single $500 million multi-year purchase of Windows and Microsoft Office, they were able to persuade the vendor to deliver more secure software on 550,000 computers. The US Government spends over 800 times that much (a total of $80 billion each year) on information technology products and services. Leveraging a larger fraction of that $80 billion in security-focused public-private procurement partnerships can transform the security of the federal government and spill over to help the rest of the American computer users.

There are people who don't want the government to do what the Air Force did, and they use misleading statements to make their case. One of the false statements you may hear has been expressed many times by vendors who don't want to upgrade the security of their products. Box 2 provides the details.

Misleading Statement 2

"The federal government should not be telling industry how to secure its products. They do not know as much about security as the vendors do, and federal meddling will stifle innovation."

If industry actually knew how to secure systems better than the government did, Google would not have called the NSA when it was infected. It would have called one of the commercial companies whose Washington reps argue so strongly that government is incompetent at determining how computers should be protected.

The visceral antagonism to government specifying security for products it buys can damage the vendor just as much as it damages national security. The best illustration is from battle Microsoft waged to stop the government from specifying secure configurations for the software it purchased.

In 2002, the Government Information Security Management Act (GISRA) was sun-setting; that's what led the House Government Reform Committee to draft FISMA. A big controversy in the FISMA drafting process was whether to empower agencies to establish standard security configurations for the systems they operate and purchase. Both major IT industry associations fought the idea of government-specified configurations for many months. During the negotiations, Frank Reeder and I asked the president of one of those associations to discuss the issue over lunch. Frank had served as Assistant Director of OMB, led the Reagan Administration team that secured passage of the Computer Security Act of 1987, and served as Assistant to the President for Administration in the Clinton White House. We both asked the association CEO why he would not support government-defined secure configurations. After nearly an hour of discussion he said, "It is the right thing to do; but if I support it, Microsoft will kill me."

The IT associations continued to fight the concept of minimum security configurations for another two years, right up until the time of Gilligan's agreement. After that, Steve Ballmer personally monitored the project, and senior Microsoft executives spoke glowingly of the value of the more secure configuration of their software and fully supported government-wide adoption of the standard that was called the Federal Desktop Core Configuration.

So if standardized secure configurations were a wonderful idea in 2005 why were they a terrible idea from 2002 to 2005. The answer, I believe, is that the Washington reps got it wrong. They hurt Microsoft's business by fighting the idea of a safer standard version of Windows. Three additional years of being known as the company that sold very insecure software to federal agencies opened the door wider for UNIX to gain market share in government and also drove many government organizations into the arms of early cloud vendors like Citrix.

Government has to take the lead in specifying security settings not because it is smarter, but because only government (NSA, DoD, DHS, FBI, and the Secret Service) has access to the forensics and attack information that shows comprehensively how attacks are actually carried out. Almost everyone else is guessing. (The one non-government exception is VISA that has collected data about how credit card data thefts are carried out.)

So when you hear the Washington vendor reps and industry association reps telling you that government doesn't know how to secure systems, just remind them whom Google called when they needed help securing their systems.

One sad footnote must be added to the story of the Air Force's great procurement success. It has not yet been replicated in most other agencies. A lack of urgency, competence and leadership combined to grasp defeat from the jaws of victory. The new White House Office of Cyberspace Policy, acting in concert with OMB, can solve the problems very quickly. It is a perfect case study of why your bill and your continuing oversight are so essential.

Using Procurement to Enable Next-Generation Dynamic Defense

State Department's continuous monitoring tools generally collect data every day or two or three. The next generation of continuous monitoring will collect data almost continuously. To make that possible, NSA and NIST are creating standard protocols for security data and are working to help software vendors who sell to DoD and the federal government build in capabilities for minute-by-minute continuous monitoring using those protocols. These protocols, called S-CAP for Security Content Automation Protocols, must be imbedded in the software that comes with computers rather than being bolted on later. The government's strategy is to publish the protocols and then provide incentives to persuade software and hardware vendors to insure their tools are S-CAP enabled. The best incentive is a combination of Department of Defense and federal civilian government buying power. That creates a big enough market to enable IT vendors, system integrators, and ISPs to embed the necessary capabilities at costs that can be spread over many large clients. This is the same strategy as that used by the Air Force to buy secure versions of Windows. The strategy makes improved security profitable for the vendors and affordable for the user organizations.

The Manpower Imperative and the US Cyber Challenge

Dynamic security can stop many attacks, but not all of them. Some will get through. A lot of highly specialized people with advanced technical security skills are still needed. They are needed throughout government and industry to do deep packet inspection, and log monitoring, and disk forensics to find the attackers that get through the defenses; to reverse engineer malicious code that is found; to perform inspections of capabilities through penetration testing; and to audit automated and manual security operations. They are needed in every development organization to architect security into new applications and to write code that is free of security flaws. They are needed as security-savvy system administrators who can recognize and flag anomalies and become a human sensor network. They are needed in the military to find vulnerabilities in commercial software and hardware before adversaries do, to build new exploits, to conduct military operations. People with any of those skills are VERY rare and in high demand.

> *"There are about 1,000 people in the US who have the specialized security skills to operate effectively at world class levels in cyberspace. We need 10,000 to 30,000."* ***(Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA's Clandestine Information Technology Office, The Pentagon, October 3, 2008.)***

Security skills shortages extend from the federal government to the US defense industrial base, federal information systems contractors, utilities, telecommunications companies, and most other segments of the critical national infrastructure. In fact, wherever senior management has been made aware of a major, damaging cyber attack, the shortage becomes immediate and acute. For example right after Google got hacked and learned from the NSA what it takes to find evidence of the advanced persistent threat, reports filtered in from all around the US that Google was searching for strong specialized security talent. Sadly the talent shortages for people with specialized security skills are so acute that if Google gets one, some defense industrial base company probably loses one from a critical project. Highly skilled security people will be the most sought after weapon in any future war. Our nation needs to build a pipeline to fill the gap of 20,000 to 30,000 cyber guardians.

For the most part, our colleges cannot create the needed talent because the faculties in the vast majority of colleges are not skilled enough in the specialized, hands-on security tasks to be able to identify and nurture world-class talent. The US Cyber Challenge is the principal initiative aimed at filling that void. It uses five different progressively more challenging competitions, most of them on line, to entice and challenge and nurture talented young Americans. Thousands of young people have entered the competitions since the U.S. Cyber Challenge was announced 11 months ago, and many very-talented young people are being identified and supported. The program is now directed by Karen Evans who previously served as Administrator of e-Government at OMB. She has been doing an extraordinary job of getting industry support and leading the college faculties and state agencies and volunteers who are staffing summer cyber camps in Delaware, New York and California. Senator Carper deserves special thanks. He has given generously of his time to recognize winners and has empowered his staff to help the state employees and college professors make the Delaware Cyber Challenge very effective.

Your support for the US Cyber Challenge in S 3480 will go a long way toward closing the skills gap. If you add the small change I mentioned earlier for language in section 404, to make sure contractors with technical responsibilities must prove they have the right specialized skills to do the assigned jobs effectively, you'll have a huge impact on enabling the government to protect its systems.

The Bottom Line

By enacting the legislation before you, with a few small amendments to address the shortcomings I outlined, Congress can immediately change the way the cyber-security game is played to the benefit not just of government, but of the economy and the American people.

Thank you for your service and efforts on our behalf and for this opportunity to share my views with you.

Statement of
Steven T. Naumann
Vice President, Wholesale Market Development, Exelon Corporation
On Behalf of the Edison Electric Institute and the Electric Power Supply Association

Before the
Homeland Security and Governmental Affairs Committee
United States Senate

June 15, 2010

Mr. Chairman and Members of the Committee:

My name is Steve Naumann, and I am Vice President for Wholesale Market Development for Exelon Corporation. I have participated on committees, task forces and working groups of the North American Electric Reliability Corporation (NERC) and recently completed serving as Chairman of NERC's Member Representatives Committee. I appreciate your invitation to appear today to discuss securing the North American electric grid against cyber threats, and the opportunity to testify about the Protecting Cyberspace as a National Asset Act of 2010. At the outset I would like to thank Chairman Lieberman, Ranking Member Collins and Senator Carper for the thoughtful approach taken in the bill and for your leadership on this issue.

Exelon is a holding company headquartered in Chicago. Our retail utilities, ComEd in Chicago and PECO in Philadelphia, serve 5.4 million customers, or about 12 million people – more than any other electric utility company. Our generation subsidiary, Exelon Generation, owns or controls approximately 30,000 MW of generating facilities, including fossil, hydro, nuclear and renewable facilities. Our nuclear fleet consists of 17 reactors; it is the largest in the nation and the third largest in the world.

I am appearing today on behalf of the Edison Electric Institute (EEI) and the Electric Power Supply Association (EPSA). Exelon is a member of both. EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members worldwide. EEI's U.S. members serve 95% of the ultimate customers in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. EPSA is the national trade association representing competitive power suppliers, including generators and marketers. EPSA members own 40 percent of the installed generating capacity in the United States, providing reliable and competitively priced electricity from environmentally responsible facilities.

Both EEI and EPSA also are part of a broader coalition of electric power stakeholders. While I am not officially testifying on its behalf, this coalition includes several major trade associations representing the full scope of electric generation, transmission and distribution in the United States, as well as regulators, Canadian interests and large industrial consumers. Rarely do these groups find consensus on public policy issues, but in the case of securing the electric grid, there is near unanimous support for a regime that leverages the strength of both public and private sectors to improve cyber security.

My testimony focuses on the value of this cooperative relationship, the unique nature of threats to the power grid, and the ongoing efforts of the Nation's electric sector to respond to those threats. I also will share observations related to the Committee's bill, particularly appreciation for its adherence to three principles the industry believes are integral to successful cyber security policy. These include:

- Leveraging public and private sector expertise, while including robust information sharing between government and the private sector, as well as among other stakeholders;
- Limiting the scope of any new authority to emergencies that will affect truly critical infrastructure; and,
- Addressing threats and vulnerabilities in a comprehensive way, including a multi-sector approach that uses a government-wide coordinator to deal with the various critical infrastructure sectors.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and electric utilities in ensuring the cyber security of the nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for ongoing consultation and sharing of information between government agencies and utilities.

Fundamentally, however, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of limitations on its access to classified information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. Thus the government is able to detect threats, evaluate the likelihood of a malicious attack and the risk of an attack and utilize its expertise in law enforcement. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operate. Owners, users, and operators of the electric grid are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation, including ensuring against unintended consequences of remedial actions. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more secure system for our customers.

Thus, the industry appreciates that greater cooperation, coordination and intelligence sharing between government and the private sector is built into the Committee's legislation that we are discussing today.

I would add that simply creating mechanisms for information sharing is only part of the solution. Those lines of communication must be developed at the highest levels of both government and industry, and then drilled on a regular basis to ensure that, in times of crisis, those with relevant information and operational expertise can communicate seamlessly, quickly and when needed, securely.

Another important component is your legislation's narrow scope; it focuses appropriately on the need to protect truly critical assets. There is a security axiom that states: if you try to protect everything, you protect nothing. Put another way, the risk-based prioritization reflected in the proposed bill ensures both government and private sector resources are allocated wisely.

Exelon, for example, is addressing the risks we know about through a "defense-in-depth" strategy while appropriately balancing considerations of potential consequences. This defense-in-depth strategy includes preventive monitoring and detection measures to ensure the security of our systems. We perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform us about whether our preventive strategies are working so that we can enhance our protection as technologies and capabilities evolve.

Reinforcing the need for a private sector role in threat mitigation, these penetration tests, which allow us to practice and enhance our monitoring capabilities, also yield lessons learned that are unique to our system. Because no two power companies have identical network, hardware or logistical configurations, no single entity will know our system's strengths or weaknesses quite like we do. The legislation recognizes these different characteristics of our systems by authorizing the Director of the National Center for Cybersecurity and Communications to approve alternative measures submitted by owners or operators to protect critical infrastructure against the threat.

The industry believes new emergency authority to address imminent cyber security threats is appropriate. I want to emphasize, however, that current law already provides the means to address many cyber security issues in the electric industry. Section 215 of the Federal Power Act (FPA), which was enacted by Congress as part of the Energy Policy Act of 2005, provides for mandatory and enforceable electric reliability rules, specifically giving the Federal Energy Regulatory Commission (FERC) oversight authority over cyber security rules.

The basic construct of the relationship between FERC and NERC, which FERC certified as the Electric Reliability Organization (ERO) under FPA Section 215, in developing and enforcing reliability rules is sound. In summary, NERC, using a well-defined stakeholder process that leverages the vast technical expertise of the owners, users, and operators of the North American electric grid (including those in Canada with whom we are interconnected) develops reliability standards, which are then submitted to FERC for review and approval. Once approved by FERC, these standards are legally binding and enforceable in the United States. NERC also submits these standards to regulatory authorities in Canada.

I applaud the Committee for addressing what additional authority is needed to promote clarity and focus in response to imminent cyber security threat situations. Legislation in this area should complement, not supplant, the mandatory reliability regime already established under FPA Section 215, and any new government authority should be appropriately narrow and focused only on unique problems that cannot be addressed under Section 215. The FPA Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation.

The importance of government-industry cooperation and consultation cannot be overstated. Any cyber security legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. Consultation is critical to improving cyber security.

Furthermore, every power company operates different equipment in different regulatory environments, making it difficult to offer generalizations about the impacts to the bulk power system or costs and time required to mitigate any particular threat or vulnerability. Costs in particular are an important part of the equation, as the uncertainty associated with federally directed cyber security orders, where the scope of an attack and the required remedies are an unknown and thus cannot be planned for, creates an outstanding question related to economic feasibility and capability. This complexity underscores the importance of consultation with owners, users, and operators, as well as state and federal regulators, and where time permits, prior consultation, to ensure that any mitigation that may be required appropriately considers these factors to ensure an efficient and effective outcome.

For the foregoing reasons, any new legislation giving additional statutory authority should be limited to true emergency situations involving imminent cyber security threats where there is a significant declared national security or public welfare concern. In such an emergency, it is imperative that the government provide appropriate entities clear direction about actions to be taken, and assurance that those actions will not have significant adverse consequences to power operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

Finally, I would like to extend thanks for your vision to address cyber security using a comprehensive, multi-sector approach. While EEI, EPSA and Exelon's interests lie with protecting the electric grid, the interconnected nature of critical infrastructure prevents us from claiming victory unless a comprehensive approach is taken. Electric utilities, for example, rely on telecommunications systems to operate the grid, pipelines to fuel our generation, and wholesale markets to sell our product. Should any of these critical sectors be compromised, the electric grid would be impacted as well. Likewise, each of these sectors relies on the electric grid for the power they need to operate. Your bill recognizes this truth, as did the President's "60-Day Cyber Review" completed last year. I would urge the Congress to follow your leadership and approach this issue in a holistic manner.

Conclusion

While many cyber security issues already are being addressed under current law, we believe it is appropriate for the government to address cyber security in a situation deemed sufficiently serious to require a Presidential declaration of emergency. In such a situation, the legislation should clarify the respective roles, responsibilities, and procedures of the federal government and critical infrastructure industries, including those for handling confidential information, to facilitate an expeditious response.

Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation for developing reliability standards. Any new authority also should be narrowly tailored to deal with real emergencies; overly broad authority would undermine the collaborative framework that is needed to further enhance security.

Promoting clearly defined roles and responsibilities, as well as ongoing consultation and sharing of information between government and the private sector, is the best approach to improving cyber security. Each cyber security situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the electric grid.

Exelon and other electric power stakeholders remain fully committed to working with the government and industry partners to increase cyber security and appreciate the efforts of this Committee to advance legislation that would create such a framework.

Thank you again for the opportunity to appear today; I would be happy to answer any questions.

TESTIMONY OF
SARA C. SANTARELLI
VERIZON COMMUNICATIONS

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

"PROTECTING CYBERSPACE AS A NATIONAL ASSET:
COMPREHENSIVE LEGISLATION FOR THE 21ST CENTURY"

JUNE 15, 2010

Mr. Chairman, Ranking Member Collins, and members of the Committee, thank you for this opportunity to discuss the important topic of cyber security. My name is Sara Santarelli and as Verizon's Chief Network Security Officer my primary responsibility is to ensure the integrity of Verizon's network systems, including risk management, threat detection, and incident response.

The Committee's interest in cyber security is timely and crucial to the security of our nation. As a provider of communications services to millions of customers around the world, Verizon addresses cyber attacks daily and has developed a wide range of measures intended to help protect our network and the networks of our customers. But this is not a fight that should be left solely to the private sector—there is a very important role for government in securing cyberspace and we applaud the Committee's efforts to help bring clarity and definition to that role.

The legislation you have proposed represents a positive step forward in building a stronger bond between the public and private sectors with respect to cyber security. While we may not agree with some of the finer points in the bill and look forward to working with your staff to iron out those differences, we feel that the majority of the legislation supports the common goal of creating a much safer online environment for our customers and for the nation. We appreciate the difficulty you face in crafting legislation that is constructive and useful for increasing our nation's security in cyberspace, while also not placing an undue burden on private companies, large and small, that are struggling in the current economic downturn.

My testimony gives you a brief background of what cyberspace looks like from our point of view and provides several examples of actions we've taken over the past few years to address and mitigate online threats. It identifies how we believe a strong partnership between the private companies that own and operate the networks that make up cyberspace can be established with government agencies that are responsible for providing for the security of our nation against all threats, including those in the virtual world.

Verizon manages thousands of voice, video, and data networks at the local, regional, national, and international level. Ours is a global backbone network that carries large volumes of the Internet's traffic, one of the many thousands of independently owned and operated networks that make up today's global Internet. Verizon's data network includes more than 633,000 route miles of terrestrial and undersea cable, spanning six continents, and reaching customers in more than 2,700 cities and 150 countries. We provide communications services to tens of thousands of businesses and government agencies around the globe, including 97 percent of Fortune 500 companies and roughly 10 million residential broadband customers here in the United States.

Given the nature of our business, cyber security is vitally important to us. The Internet is not centrally controlled or managed. Rather, it is a globally distributed network-of-networks linked solely by implementation of a few common Internet protocols. It imposes virtually no barrier to any person seeking to reach a global audience.

But as with many technologies, the same capabilities that make the Internet a useful tool for those with good intent can also be used by those with harmful intent. The number of people connected to the Internet is estimated by some to exceed 1 billion, and not all of them have good intentions. The Internet allows for the rapid adoption of useful software applications that enhance users' lives, but it also allows for the dissemination of harmful viruses that destroy and steal data. It allows for consumers and companies to interact more efficiently with one another, but it also could be used to attack and disrupt commercial transactions. The cross-border nature of the Internet magnifies its potential for good but also complicates law enforcement.

This is the reality Verizon deals with every day. As a result, Verizon engages in a wide range of activities to enhance cyber security for ourselves, our customers, and other users of our network. These activities take place at many different layers within our organization. For example, before even deploying our network, we work closely with our vendors to help ensure that their products are able to meet our security requirements. Our network security group manages security on our networks using a variety of tools, security sensors, and other technologies to identify and mitigate threats on the Internet as they are emerging. We take action daily to address spam, phishing, denial-of-service and other malicious activity that threatens to disrupt our network or our customers' use of it. We invest in advanced threat detection and mitigation technologies. We also make strategic R&D investments to develop new technologies that deal with emerging and future threats.

In addition to addressing cyber security issues in our network core, we offer a wide range of services to help customers secure their networks and data. Services such as managed firewall, intrusion detection, intrusion prevention, and encrypted virtual private networking help customers keep their networks safe. Verizon's Government Network Operations and Security Center provides federal agencies with a single point of contact to obtain products and services to meet network operations requirements and related security matters, putting both network and security operations under one umbrella. Our security-certified data centers offer enhanced security features for customer systems and data. For residential broadband customers we offer parental controls, anti-spam features, and other security software to assist them in securing their computers.

Going beyond our network services, we offer a wide range of professional services to include security consulting, network analysis, incident response, and computer forensics. Our professional security engineers hold over sixty different certifications and federal clearances, and are available 24/7 around the world to assist customers in responding to breaking cyber security incidents.

When it comes to the security of critical networks and systems, we practice what we preach. Within our own enterprise, network-connected systems are inventoried and assigned a criticality score based on the sensitivity of the data they contain. They are then scanned periodically to identify security vulnerabilities. The results of the scanning activity are correlated to threats and system value, and the results are automatically displayed in real time on our internal system security dashboard. This real-time threat and vulnerability information about our own corporate systems has proved invaluable to our internal business leaders in helping them identify affected systems and establish priorities for remediation. Internal groups actually compete against each other to see who can consistently maintain the cleanest scorecard!

Our backbone security activities redound to the benefit of all of our users at no charge. We spend thousands of hours each year analyzing data collected from our involvement in cyber security events which, after rigorous scrubbing to remove any attribution, we publish, free of charge, in our annual data breach investigation report (DBIR). This report, which uses a Verizon-developed information-sharing framework called VERIS that we have also published as an open-source initiative, provides valuable advice and guidance for enterprise and government customers on tangible, effective steps they can take to better secure their networks today. The bottom line for Verizon is that unless our networks add value, our customers won't use them. Customers who are assailed by denial of service attacks, spam, phishing, identity theft, network scanning, hacking, and other criminal activity won't be customers of ours for long. They will quickly move to a network that is better protected.

Finally, we view ourselves as being a leader in the larger cyber security community. Verizon and other companies within the communications sector have a long history of cooperation in emergency preparedness and assisting law enforcement, to the extent authorized by law. This history distinguishes the sector from most other critical sectors identified in the National Infrastructure Protection Plan and is a reflection of our relationship with the federal government and the public policy community. The sector personifies cooperation and trusted relationships, which has resulted in the delivery of critical services when emergencies and disasters occur. This strong bond between the private and public sectors exists today in large part because of several organizations that were created in response to earlier threats to the nation's critical infrastructure. Some of the organizations that Verizon has a leadership role in or is a significant participant in include the President's National Security Telecommunications Advisory Committee (NSTAC), the National Coordination Center for Telecommunications (NCC), the Communications Sector Coordinating Council (C-SCC), the National Security Information Exchange (NSIE), and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC).

Security events are a constant reminder that our networks and our customers' networks are under a steady assault from individuals, groups, and organizations that intend to do harm. And it is important to note that these assaults are constantly changing and evolving as criminals and hackers develop new techniques to get around the latest defenses. Once launched, these assaults can escalate with astonishing speed. Improvements in computer processing power, memory, and bandwidth not only help support new lawful applications like VoIP and streaming video, but they also enable hackers to wield tremendous weapons in cyber space. Distributed virtual computer networks known as botnets can flood victims with vast amounts of traffic, send millions of spam messages to ensnare new victims, and serve as a virtual hosting network for illicit commercial activity. Government regulation of private sector network security activities must not diminish the flexibility, speed, and independence that network providers find essential in waging war on cyber crime.

In recent years, we have faced many cyberspace challenges as the four examples that follow demonstrate. In each of these cases, we have worked with other parties (providers, companies, the government, and others) to quickly address the issue at hand. Any new requirements must continue to afford us the flexibility and speed to continue resolving problems as we have in the past.

- Several years ago a major financial services institution was under a significant distributed denial of service attack that effectively disabled its ability to handle online transactions via the Internet. We worked closely with another large Internet backbone provider to quickly bring the attack under control and to help restore stability to the customer's network. We would not have been able to address the issue at hand as quickly and successfully if we had been required to brief and share information with outside parties on a real-time basis or wait for feedback on, or concurrence with, our plan of action.

- The SQL-Slammer worm was launched on January 25, 2003, at approximately 12:30 a.m. EST, and began rapidly spreading across the Internet. At that time, this worm was the fastest spreading computer worm in history, doubling in size every 8.5 seconds. The scanning technique used by the Slammer worm was so aggressive that it quickly interfered with its own growth. Within three minutes the worm achieved its full potential (with more than 55 million computers being scanned per second), at which point its growth rate slowed. Slammer infected more than 90 percent of vulnerable hosts within 10 minutes. This rapid spread caused significant disruption to financial, transportation, and government institutions. Success in stopping the Slammer worm was predicated on the ability to take fast and decisive action without extraneous briefings, consultations, or declarations.

- The recent Conficker worm experience illustrates how important it is to maintain flexibility in any cyber regulatory regime. Conficker has spawned one of the most successful and robust criminal botnets in history. It was first released on November 21, 2008, just weeks after publicity about a critical software vulnerability affecting operating systems used in a large portion of the computing infrastructure on the Internet. In response to this threat, an international working group—the Conficker Working Group (CWG)—was formed. It consists of thirty named members and many more partners and contributors around the world, including Verizon. This global partnership involved industry, governments, and educational institutions. Its efforts have largely prevented the monetization of this criminal botnet and hampered its spread at key points in its evolution. It bought additional time for more sites to fix vulnerabilities by implementing additional security controls. This botnet remains a clear threat to the world's networks and those responsible for releasing and controlling it are still at large after almost two years. Conficker is a good example of a complex and rapidly evolving threat for which existing information sharing activities have proved effective. The data and expertise needed to counter cyber threats such as this are distributed globally among companies, universities, and governments. When those groups work together, the result is greater than the mere sum of the parts. It is imperative that any government-directed information sharing mechanism be nimble and flexible enough to accommodate any and all comers, and not otherwise place restrictions or requirements on the free flow of information about the Internet.

- The Rinbot incident in 2006-2007 highlights the damage that can be caused when an average miscreant armed with powerful hacking tools that are widely and cheaply available on the Internet "black market" takes aim at just a few critical vulnerabilities in unpatched systems connected to the Internet. Security sensors deployed in Verizon's Internet backbone network alerted our network security teams to an emerging outbreak. We disseminated this information quickly within the company, to customers, to the impacted vendor, and to numerous established cross-industry groups. Verizon's information helped prioritize the identification, mitigation, and ultimate takedown of the Rinbot botnet. Although the aggressive nature of this virus led to the complete shutdown of a regional hospital network in Canada and several enterprise networks in the United States, we believe that quick action by Verizon and others helped prevent far greater harm.

Headlines often make it appear that the Internet is so vulnerable and open to attack that nothing can be done or is being done to safeguard consumers and our country. But what these events illustrate is that public and private sector response and remediation activities and information sharing exist today in ways that are highly advanced and effective, and that speed and flexibility are essential for combating such cyber threats. Even without government mandated information sharing and oversight, private sector operators are—and have been for years—moving "full speed ahead" to expand their tools, expertise, and capabilities necessary to identify threats, address them, and preserve providers' ability to serve their customers.

That's not to say there is not a role for government—there is. The government is uniquely positioned to do things the private sector simply can't. For example, the government has the power to:

- Share unique and valuable information resources that it possesses which might aid private-sector cyber security efforts;
- Work with industry to define mutually-agreeable plans for addressing potential incident scenarios before such incidents occur;
- Incent those who are slow in adopting cyber security best practices to improve their security posture, thus reducing the negative externalities that exist from the under-investment by some in adequate network security;
- Secure its own networks and systems, thus protecting some of our nation's most critical information assets;
- Facilitate the development of new security offerings by requiring best-of-breed security features in the products it purchases;
- Provide valuable incentives for desirable private action, such as limitations on liability for collateral damage flowing from otherwise desirable network security behavior;
- Clear away outdated legal barriers that impair some of today's cybersecurity activities; and
- Work with other governments, to persuade regimes that are havens for cyber criminals to take a firmer stand in support of global Internet security.

With this in mind, we believe government efforts should be focused on the following key goals and objectives, most of which are addressed in the proposed legislation:

- Centralize and clarify government roles and responsibilities. The government needs to speak with one voice when setting national priorities and agendas. Proposals in this bill such as the Office of Cyberspace Policy and the National Center for Cybersecurity and Communications, for example, could streamline interactions and ensure consistency in the government's view and in the security of its own infrastructure.

- Avoid duplication of cyber security initiatives. Given the wide-spread level of concern across all government sectors on cyber security issues, it is not surprising that many different proposals exist for how to best address it. Unnecessarily duplicative or inconsistent initiatives threaten to drain scarce resources, and divert us from substantive cybersecurity activity. This bill takes several steps towards achieving the goal of reduced duplication of initiatives, and we appreciate the effort that this will take.

- Promote enhanced security for private sector infrastructure while maximizing private sector flexibility and preserving speed of response. Clearly, there will always be those who are slow in adopting best practices in the area of cyber security. It is appropriate for government to provide strong incentives for those enterprises to enhance their level of security. Given the wide range of networks and technologies, as well as the rapid pace with which cyber threats are ever-evolving, it is imperative that we do not lock ourselves into a single regulated approach. Owners/operators of critical infrastructure must retain the freedom to implement any and all measures available to them to secure their infrastructure and critical systems. With respect to speed-of-response—speed that is often measured in seconds, not hours or days—it is essential that providers have the freedom to take decisive action to protect their critical cyber resources without being subject to regulatory second-guessing. Unfunded regulatory mandates and command-and-control type governance structures must be avoided. The most effective approach, which appears to be the direction that this bill is taking, is a public-private partnership where government provides assistance and expertise to the private sector, coupled with incentives like confidentiality and liability protection to encourage the private sector to implement desired activities and with freedom to take decisive actions.

- Drive diplomatic efforts to reduce the number of countries that are havens for cyber criminals. While this legislation does not directly address international diplomacy, it does recognize that it is one of the key objectives of any national strategy to increase the security of cyberspace.

- Remove outmoded legal barriers to appropriate information-sharing. A number of outdated laws present barriers to the collection, use, and sharing of information by network operators and their customers, and the government. We urge you to update this patchwork of laws and provide a coherent legal framework that takes into account the current state of technology and strikes the appropriate balance between privacy and the need for information sharing among government and the private sector.

We look forward to working with you and your staff on further refining these mechanisms to ensure that network service providers and other private sector actors retain the freedom to act quickly as they see fit to address these ever-evolving and rapidly spreading threats to our networks, our economy, and our way of life.

Mr. Chairman and members of the Committee, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing critical infrastructure information systems. I look forward to answering any questions you may have.

Testimony of Robert D. Jamison, Former Under Secretary of the Department of Homeland Security for the National Protection and Programs Directorate

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

Hearing on "Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century" June 15, 2010

Chairman Lieberman, Ranking Member Collins, Senator Carper and Members of the Committee, I appreciate the opportunity to testify before the Committee on the issue of Protecting Cyberspace as a National Asset. I also appreciate the Committee's continued interest and activities in this vital area of national and homeland security.

Today, I will share with you my perspective on some of the key issues surrounding how we secure cyberspace and how I think your legislation can assist the effort. As you may recall, I have a diverse private sector, not-for-profit, and government background that impacts the way that I look at the complicated issue of cyber security. I spent over fifteen years at the United Parcel Service and the American Red Cross in senior management roles. This experience in the private and non-profit sector prepared me to enter government service during the last administration. I began my career in government service with the Federal Transit Administration at the Department of Transportation under the leadership of Secretary Norman Mineta. In addition to my normal duties as Deputy Administrator of FTA, I also had the opportunity to work helping to lead the Department's recovery efforts in lower Manhattan immediately after the September 11th attacks, as well as lead the Department's transit security efforts. That work led to my transition to the Transportation Security Administration (TSA) at the Department of Homeland Security (DHS), as the Deputy Assistant Secretary.

I was then confirmed by this Committee to lead the National Protection and Programs Directorate at the Department of Homeland Security. NPPD was a DHS component in transition from Preparedness Directorate to a risk-based, resiliency organization dealing with the critical issues of identity management, infrastructure protection, and cybersecurity and communications.

In this capacity, I led the Department's efforts in the area of cybersecurity and communications. I was the senior Department official who assisted in the drafting of HSPD-23 and the Department's implementation of the Comprehensive National Cybersecurity Initiative (CNCI). What I found when I arrived at NPPD in April of

2007 was an organization at a crossroads. The National Cybersecurity Division was staffed with bright hard working people tasked with the mission of securing our Federal government networks and working with the private sector to secure our nation's critical infrastructure and key resources. The US-CERT – United States Computer Emergency Readiness Team – had a small government staff and the tools they had deployed to detect malicious activity on our government networks were looking at flow analysis – but only after the fact. This limited capability, deployed on less that 40 of the civilian government's internet access points, augmented the security efforts of less than 1% of the government's internet traffic and data communications.

The Comprehensive National Cybersecurity Initiative had a dramatic impact on this limited DHS role. Not only did it solidify a common government strategy consisting of twelve specific initiatives across government aimed at improving our nation's cybersecurity and communications posture. It launched an execution plan to put our critical networks in a more defensible posture and initiated the deployment of critical automated monitoring capabilities and the dynamic, real-time sensors needed to defend against our cyber adversaries. It also, as you know, called for a more robust DHS cybersecurity role similar to its role in other homeland defense areas; outlined education and awareness programs; required supply chain security strategies, and much more.

The CNCI and the subsequent Cyberspace Policy Review ordered by President Obama acknowledge cybersecurity as one of the most pressing national security areas in a generation. And it called on the government, private sector, academia, and our international partners to work cooperatively together to begin to take the necessary steps to enhance the cybersecurity of our nation.

Cyber Landscape

If you scan the cyber landscape today, what you find is a very diverse operating environment for an agency like DHS. An environment composed of operational networks, informational networks, and customer focused organizations with databases full of personal identifiable information.

You need only look to the Federal government to see we have multiple agencies with different missions, networks, authorities, and capabilities. US-CERT at DHS is primarily focused on operationally securing the dot gov networks. The Department of Justice is not only concerned with the law enforcement aspect but also the legal authorities that any agency has to execute its mission. The Department of Defense and the National Security Agency are focused on protecting our military networks, employing offensive measures, and determining what constitutes an act of war in cyberspace and how our government responds. The Department of State is focused on our international efforts. Department of Commerce is working on several fronts including issuing standards and guidelines through the National Institute of

Standards and Technology and working with the National Science Foundation and National Telecommunications and Information Administration on the educational, research, and governance fronts.

All of the Federal agencies are responsible for the protection of their respective networks and many, like the ones mentioned above, have responsibilities as it relates to our national cybersecurity strategy. Our Federal department and agencies are all on different evolutionary paths of cyber readiness and defense. Yet, they must all work together, cohesively and in partnership, to improve our nation's ability to prevent, detect, and respond to the cyber threats facing our great nation. The executive branch must continue to work with Congress to ensure we are on the right path in securing this vital national asset. And together we must ensure that as we proceed in this arena we are taking privacy and civil liberties in account at every step.

The Bill

As Under Secretary of the National Protection and Programs Directorate, I was faced with many challenges and some persistent obstacles. My directorate in many ways did not have sufficient infrastructure in place to sustain the growth mandated by the Comprehensive National Cybersecurity Initiative (CNCI). The bill introduced last week by the Homeland Security and Governmental Affairs Committee directly addresses many of the challenges I faced and has the potential to leave the Department of Homeland Security better positioned with the necessary tools to execute its mission.

I believe one of the most important parts of the bill is the clarification of authorities, roles and responsibilities of various departments and agencies.

While conducting my duties as the senior official at the Department of Homeland Security on cybersecurity and communications issues, I can honestly tell you that I had authority I needed and the support of the leadership from DHS and the interagency. It may be old school, but I always encouraged my staff to step into the authority as outlined in HSPD-23 and execute the mission accordingly. However, I found it challenging at times to motivate my staff to embrace this charge. They often told me that they lacked the definitive clarification of authority to execute their mission and this sentiment was often echoed by many of our interagency partners. Sometimes you need that conviction of authority to drive the necessary actions and acceptance of the responsibility.

This seemingly minor nuance of authority and roles is a critical piece that must be addressed to position DHS for continued success. DHS and its partners have critical work to complete. We must ensure that we have the mechanisms in place to ensure that the nation's strategies are current and effective and ensure the rights of our citizens. **However, continued debate of roles and responsibilities and the reevaluation of cyber policy is delaying the execution of the most important**

issue facing the United States government when it comes to cybersecurity: the continued consolidation of internet access points and ramped up deployment of dynamic, real-time sensors and capabilities that will position government networks to be more effectively defended. Your legislation goes a long way to putting these authoritative issues to rest. It is clear that Federal civilian departments and agencies must work with the new National Cybersecurity and Communications Center at DHS to secure our government networks.

One of the most important management fundamentals that I have adopted in my professional career is ensuring the implementation an effective performance measurement and management program. Good performance management and the use of quality metrics have the potential to rapidly drive progress in both the private and public sector.

The capabilities that DHS and the government are deploying will result in an improved defensive posture and a much-improved situational awareness picture across the government domain. Commonly referred to as Einstein 2 and Einstein 3, these systems will also uniquely position DHS to have access to real-time network performance data that will be critical to driving compliance, spurring continuous improvement, and detecting anomalous network behavior.

With these systems, DHS will now be able to show Federal departments and agencies another perspective on their networks. DHS will be able to provide them with individual agency data, comparitive data from the dot gov networks, and data from the private sector and our international partners. This comprehensive common operating picture will help to inform the CIOs and CISOs on what network security measures need to be evaluated and taken throughout their enterprise architecture. It significantly raises the baseline of cybersecurity across the Federal government. Having a performance management system to take advantage of that data is the key to success.

The Federal Information Security Management Act (FISMA) requires many practices that are fundamental to good network security such as inventory management, change management protocols, documentation, and testing. However, measuring network performance and security should be continuous and timely. Your bill allows us to move from a delayed audit based approach to the utilization of more timely, operational, and actionable information. It moves us from an annual "snapshot in time" approach to a continuous monitoring approach for the security of our networks with the performance responsibility resting with the cabinet level appointee, Chief Information Officer, and Chief Information Security Officer. Having the ability to look at what you call the "composite state of security" on a daily and ongoing basis will improve our defenses. And knowing and understanding the data will give us an opportunity to measure our improvement and success.

I draw particular attention to the improvement of cybersecurity for the Federal government and its systems, because it is difficult to speak with credibility to the private sector when our own systems are significantly vulnerable. The work done under the CNCI and the subsequent Cyberspace Policy Review, coupled with your legislation lays the foundation to begin a more serious dialogue with the private sector. As the government works to secure its own networks, it will concurrently work cooperatively with the private sector to enhance the cybersecurity of our nation's critical infrastructure and key resources.

Hiring and procurement authorities

Perhaps the most overwhelming challenge I faced when I moved from the Deputy at TSA to the Under Secretary of NPPD, was being able to quickly identify, recruit, and bring onboard a skilled cybersecurity workforce. While at TSA, I came to appreciate the TSA hiring authorities not only for their flexibility to allow the quick stand up a 60,000 plus workforce around the country to respond to transportation security threats, but for their ability to combine fairness with a more expeditious process. Similar flexibilities are needed to successfully execute the cybersecurity mission responsibilities at DHS, particularly as they rapidly ramp up their staffing. I can tell you from personal experience that some of my best employees and senior leaders were lured away by not only the private sector, but by other Federal agencies. It was difficult to compete with the compensation flexibility and incentives that other agencies and the private sector were able to offer. Going forward, DHS will need to heavily rely on these hiring flexibilities and incentives you have provided them to successfully execute the additional responsibilities in this bill.

The amount of time it takes to complete the hiring process, particularly the time from selection of a candidate to their first day of work was also a persistent problem. In a competitive environment, many candidates will not wait for the process to be completed. Our government must be able to not only hire the best and the brightest through an effective and efficient hiring process; but we must be able to bring them on board onto our watch floors and into our labs without an extended delay to clear the vetting and security clearance processes. Since the overwhelming majority of these jobs require security clearances, I firmly believe this issue needs to be addressed by this legislation.

The demand for cyber professionals is growing and will continue to grow. The nation must have a comprehensive hiring strategy and understand the changing demands for Federal government workers moving forward. We must get ahead of our workforce challenges and this legislation helps us do that. By asking OPM to investigate, identify and help provide solutions that agencies can use when it comes to internships, training, and part-time work, we will look to create a new generation of cyber warriors not just in Washington, D.C., but in every school and community in America. As we look at our hiring priorities as a nation, I would also encourage that we prioritize our most pressing needs and that we give the agencies with the most critical missions and staffing needs not only a focused strategy, but the competitive advantages to fill their vacancies.

Infrastructure Protection

While I was at the Department of Transportation and while Deputy at TSA I became familiar with the work of the Office of Infrastructure Protection and its important mission. As the former Under Secretary of NPPD, I more than most understand and appreciate the linkages between the Office of Infrastructure Protection and the cybersecurity mission of the Department of Homeland Security. Through the National Infrastructure Protection Plan, commonly referred to as the NIPP, our government has developed a coordinated process to work with the nation's eighteen critical sectors. I suggest, as you do in your bill, that we need to continue to support this process and the vital coordination that it brings. The NIPP allows various agency responsibilities and sector needs to be coordinated giving us a comprehensive security plan that minimizes confusion and overlapping requirements and responsibilities.

If we think about the next generation FAA program and the smart grid deployment, we quickly realize that cyber issues permeate our daily lives. Cyber issues are not limited to communications or the information technology industry. They touch nearly every aspect of our lives from the time we wake up until the moment we arrive back home. Given the omnipresence of cyber in our society, DHS should continue to leverage the Office of Infrastructure (OIP) field presence, through their Protective Security Advisors, their important sector relationships – our government and DHS in particular can use years of foundational work to leverage private sector partnership to improve cybersecurity across eighteen sectors. One need only look to the success of the industrial control systems partnership between OIP and the National Cyber Security Division or the Cross-Sector Cybersecurity Working Group to realize the criticality of the relationship between these two DHS entities. Your committee held a hearing last year about cybercrime where you heard learned that not only are we facing nation state adversaries but organized criminal enterprises who are capable of carrying out large scale cyber intrusions against many sectors including our financial sector and many small and medium sized businesses. It is imperative we work with all sectors to ensure they are improving their cybersecurity baselines to confront the changing nature of the threats.

Your bill also recognizes the important relationship between the National Communications System (NCS) and the US-CERT. The NCS mission to ensure the redundancy and resiliency of our communications networks goes hand in hand with the critical mission of network and critical infrastructure defense. By working in partnership with industry through its major carriers and with the Federal Communications Commission, DHS through the National Coordinating Center has provided a 24/7 watch communications capability for this country. This capability augments the situational awareness and defense capabilities of US-CERT to more effectively understand the full common operational picture and to defend our networks.

As the nations communications infrastructure continues to migrate to internet based communications and as the cybersecurity mission matures, we are confronted with the inevitable convergence of these two areas. I am pleased that you recognize that these mission sets are inextricably linked.

Establishment Of NCCC As An Operational Entity

The establishment of the National Cybersecurity and Communications Center as an operational component of DHS will place the necessary focus and emphasis on this mission area that it merits. As the former Deputy of TSA, I understand what it means to be an operational entity within DHS. It means not only having an operational mission, but more control over the critical support functions that are vital to your success. The mission and responsibilities of the NCCC demands that type of control. In addition, giving the NCCC hiring and procurement authority will assist their rapid growth as they step into their new responsibilities.

Before I close, I would like ask you to take a few issues under advisement. First, DHS must be careful not to divert key resources from the building of critical capabilities at the Department. I know from personal experience that the disparate demands of the mission and the magnitude of DHS's responsibilities can challenge the resources under your control. It is of vital importance that DHS maintain its focus, attention, and resources on quickly securing the dot gov domain. We must remember that it took the Department of Defense several years to ramp up their capabilities both in terms of node consolidation and the deployment of an effective perimeter defense. While their accomplishments should be commended, today, they still have work to do. As quickly as we want DHS to consolidate the nodes and establish a robust perimeter defense, we must allow them sufficient time to do it. This mission area is clearly within their capability and given the time and resources they should meet the challenges successfully.

Second, the diversity and magnitude of our critical infrastructure and key resources creates many challenges in effectively deploying capabilities and resources. This creates a resource challenge for DHS and I ask that the appropriate Congressional committees work with DHS and the Office of Management and Budget to determine what will be needed to carry out these responsibilities.

Finally, as this legislation moves through both chambers of Congress, we must remember that the dot gov defenses will and must evolve. This evolution will yield valuable lessons that will certainly impact critical infrastructure key resource standards and most likely will change and improve the requirements imposed by DHS. DHS must be nimble and build in flexibilities to its processes and procedures to account for that inevitable change.

Closing

In closing, I think this important piece of legislation will improve the ability of the U.S. government and DHS to carry out its cybersecurity mission. You empower DHS by giving them critically needed authorities in the areas of hiring and procurement. Your bill clarifies the roles, responsibilities and authorities of the Federal departments and agencies. It moves the government to end debate on who should be doing what or who can do what and mandates progress. Finally, and to me most importantly, it lays the groundwork to accelerate the ramp up of Federal capabilities necessary to protect our nation's networks and critical infrastructure.

Again, I thank you for the opportunity to testify before you and I look forward to answering any questions you may have.

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement for Chairman Joseph Lieberman
Hearing, "Securing Critical Infrastructure in the Age of Stuxnet"
Homeland Security and Governmental Affairs Committee
November 17, 2010

Good morning, the hearing will come to order. This is a hearing to both remind us and educate those who are watching about the reality of the cyber threat to the United States and how important it was that we worked hard to develop cyber security reform legislation in this committee. It's unfortunate that the clock will run out on us before we have a chance to complete negotiations with other committees and with the administration, who I regret to say did not engage as early in the process of developing this legislation as was necessary.

But this Stuxnet story really takes the reality of the threat to a new level and should awaken any skeptics. There are some who think we're overstating the threat and therefore overreacting in the public resources that we're devoting to the protection of our cyber systems here in America. Of course I totally disagree with that argument.

We have an extraordinary group of witnesses here today, who will not only tell us what Stuxnet is, but will help talk more generally about the cyber threat to our country.

I want to say, in terms of our legislation, that it's certainly my intention to come back to this legislation early in the next congress and try to get it out as soon as possible. Again, I want to say that this will require more immediate and intense concentration by the Administration and by some of the other committees that claim jurisdiction here. We of course are the ultimate source of jurisdiction for cyber security that is non-defense, which is the Armed Services Committee. This will be a real priority for the Committee when the new Congress begins next year.

<u>The Following Was Entered Into the Hearing Record:</u>

Last summer, a dangerous piece of malicious software, or "malware," was discovered that dwarfed anything that has come before it in cyberspace, both in sophistication and destructive potential.

Named Stuxnet, it specifically targets computers that run the industrial systems used to control electric, water treatment, nuclear and chemical plants, as well as pipelines, communications, transportations, manufacturing systems and other critical infrastructure.

Stuxnet is a dual menace. First, it has the power to burrow deep into a network and steal secrets. Second, it also has the ability to commandeer industrial operations and make machinery do things – like open or close a valve – undetected by a plant's operators because Stuxnet tells the operators their instructions are being followed.

The potential for catastrophic consequences should these critical systems fall under the control of our enemies is obvious. But prior to Stuxnet, many considered the probability of this kind of attack on a large-scale system to be remote.

This Committee has already held several hearings on cyber security, during which we discussed denial of service attacks that shut down commercial websites and phishing schemes that tricked people into giving away crucial information that could then be used to empty corporate bank accounts or steal industrial or national secrets.

But these attacks are primitive compared to Stuxnet – like muskets compared to a modern machine gun.

Experts estimate that 10,000 man-hours of programming time went into writing Stuxnet as a seamless piece of code, and its authors would have had to be experts both in Microsoft's operating systems and in the much more esoteric systems and computer languages that control industrial systems.

Put differently, Stuxnet was created by a team that could speak both English and Urdu with complete fluency.

Stuxnet has some 4,000 functions, not all of which have been documented yet. By comparison, the software that runs the average e-mail server has about 2,000 functions.

Stuxnet invades its target computers using four different Microsoft Windows security vulnerabilities that had been unknown until Stuxnet was set loose.

These security flaws, known as "zero-day vulnerabilities," are difficult to discover and are valuable commodities on the black market. Using four of them in one piece of malware is unprecedented.
And Stuxnet will even update itself automatically if it runs into a newer version on another computer.

Stuxnet is highly sophisticated and complex. So far, Stuxnet has done no known damage. It may still be looking for its ultimate target or, it may have already found it and is simply lying in wait for the precise set of events that will trigger its more destructive capabilities.

The very fact that Stuxnet exists means that no one can argue anymore that a cyber attack on our critical infrastructure is hypothetical or hyperbolic.

Our concern today is what Stuxnet tells us about the state of security of our critical infrastructure and what role the federal government should play in this new age of cyber warfare, where the targets will be strategic computer network systems that are almost entirely in the hands of the private sector.

This is no small difference. The private sector evaluates risk differently than the government. A single industrial network, say an electric power plant, might look at the cost of security and say: "What is the minimum I must do to protect the system and not hurt my bottom line."

Downtime is expensive, which is why the average industrial system is off line for just four hours a year for maintenance. And if a system is only rarely taken down, it is all the more difficult to install patches from newly discovered vulnerabilities.

The federal government has to take the broader view and look at how we defend the economy and the computer infrastructure that supports it as a whole and create standards to accomplish that.

Legislation Sen. Collins and I proposed, and which the Committee reported out, would give the federal government modern tools to secure and defend the nation's most critical cyber networks and establish public/private partnerships that will help set those kinds of national cyber security priorities.

Most relevant to this hearing are the provisions that would establish a National Center for Cybersecurity and Communications – or N Triple C – within the Department of Homeland Security and empower that Center to help secure critical infrastructure networks, like utilities and communications systems.

The reality is that the current, porous state of our nation's infrastructure means that it wouldn't take malware as robust and sophisticated as Stuxnet to cripple many of our critical systems.

Consequently, our legislation raises the security bar for all systems, making attacks more difficult, and putting in place processes that will help remediation after a successful attack.

I'm sorry to say it seems unlikely we can pass this bill in this lame duck session, although we should. I've been disappointed that the Administration and some other Committees that have an interest in this problem have been slow to engage.

But we have made a lot of progress on it and I hope in the next session of Congress our committee can pick up where we left off and quickly enact this legislation that is crucial to public safety and our economic and national security.

Stuxnet was the warning of a gathering storm. We ignore it at great peril.

Statement of Ranking Member
Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"

November 17, 2010

★ ★ ★

Today's hearing focuses on cyber threats to our nation's most critical infrastructure.

Much attention has been paid to cyber crimes such as identity theft and to cyber attacks intended to steal proprietary information or government secrets. But lurking beyond those serious threats are potentially devastating attacks that could disrupt, damage, or even destroy some of our nation's critical infrastructure, such as the electric power grid, oil and gas pipelines, dams, or communication networks. These cyber threats could cause catastrophic damage in the physical world.

This threat is not theoretical. It is real and present. The newest weapon in the cyber toolkit was introduced to the world in June, when cybersecurity experts detected a cyber worm called Stuxnet.

It was clear to cybersecurity experts that Stuxnet was extraordinarily sophisticated malware, whose complexity was something no lone hacker could achieve. With more than 4,000 functions, the worm's complex code was longer than much of the commercial software we use on our computers every day. The development of this sophisticated attack was likely the work of a well-financed team of experts with intimate knowledge of the targeted systems.

Stuxnet was programmed specifically to infiltrate certain Industrial Control Systems (ICS), allowing the worm potentially to overwrite commands and to sabotage the infected systems. It was discovered in July at the Bushehr power plant, Iran's controversial nuclear power facility. It was also found in systems in China, Indonesia, India, the United States, and elsewhere. More than 100,000 computers have been infected.

Industrial control systems, like the Siemens systems affected by Stuxnet, are widely used in electric power plants, water and wastewater treatment, the oil and natural gas industry, transportation, and manufacturing. Malware like Stuxnet has the potential to change instructions, commands, or alarm thresholds, which, in turn, could damage, disable, or disrupt equipment.

After four months of reverse-engineering Stuxnet, cyber experts at the Department of Homeland Security, Symantec, and other researchers concluded that this malware was capable of incredibly dangerous impacts. The *Christian Science Monitor* noted that cybersecurity experts identified Stuxnet as the world's "first known cyber super weapon designed specifically to destroy a real-world target -- a factory, a refinery, or just maybe a nuclear power plant."

If a cyber attack like this worm were launched on a large transformer on the electric power grid, for example, the impact could cascade, potentially leaving large regions of the United States without electricity, halting our economy, and undermining our national security. The cyber threat is urgent, and the consequences of a major national cyber attack could be devastating.

To develop a comprehensive approach to this national threat, Senator Lieberman, Senator Carper, and I have introduced bipartisan legislation to strengthen our cyber defenses across both the federal government and the private sector.

Unanimously approved by this Committee in June, our bill would fundamentally reshape how the federal government works collaboratively with the private sector to address all cyber threats, from espionage and cyber crime to attacks on the most critical infrastructure.

For our nation's most critical systems and assets, whose disruption would cost thousands of lives or multiple billions of dollars, the bill would establish certain risk-based performance requirements to close security gaps.

These requirements would apply to vital components of the electric grid, telecommunications networks, financial systems, or other critical infrastructure systems that could cause a national or regional catastrophe if disrupted. The owners and operators of these systems would be able to choose which security measures to implement to meet applicable risk-based performance requirements. This model would allow for continued innovation that is fundamental to the success of the IT sector.

The President's authority to deal with a catastrophic cyber attack aimed at critical infrastructure would be carefully defined -- and constrained. The President would not have the authority to take over critical infrastructure.

The Stuxnet worm demonstrates that cyber attacks reach beyond threats to identity, intellectual property, and the economy, and can produce serious, potentially devastating effects on critical infrastructure.

The Department of Homeland Security's Control Systems Security Program (CSSP) has made much progress in supporting owners and operators of critical infrastructure to address cyber vulnerabilities to industrial control systems. We must build on these partnerships.

Despite the progress made by DHS, the government's overall approach to cybersecurity remains disjointed and uncoordinated. The threat is too great to allow this to continue. The need for Congress to pass comprehensive cybersecurity legislation is more urgent than ever.

Statement for the Record
of
Seán P. McGurk
Acting Director, National Cybersecurity and Communications Integration Center
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

November 17, 2010

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee: I am Seán McGurk, the Acting Director of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) within the Office of Cybersecurity and Communications at the National Protection and Programs Directorate, and I have served for the last two years as Director of the Control Systems Security Program within the National Cyber Security Division. It is a pleasure to appear before you today to discuss the Department's cybersecurity mission and how we are coordinating with the nation's critical infrastructure asset owners and operators to reduce the cyber risk to industrial control systems.

Overview of DHS Cybersecurity Responsibilities

DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. DHS serves as the principal federal agency to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, state and local governments, and the private sector to protect domestic critical infrastructure and key resources.

DHS takes threats to our private sector critical cyber infrastructure as seriously as we take threats to our conventional, physical infrastructure because our society and our economy depend on these networks and systems to operate effectively. A successful, large-scale cyber attack could have cascading effects across many sectors and around the world, which is among the reasons why President Obama identified our digital infrastructure as a national strategic asset.

In line with the President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, DHS has developed a long-range vision of cybersecurity for the nation's homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: (1) help create a safe, secure and resilient cyber environment; and (2) promote cybersecurity knowledge and innovation.

We are moving forward on this mission and working collaboratively with our public and private sector partners to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. At the Office of Cybersecurity and Communications (CS&C), we are working to enable and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats:

1. First, we continue to enhance the EINSTEIN system's capabilities as a critical tool in protecting our federal executive branch civilian departments and agencies.

2. Second, we are finalizing the National Cyber Incident Response Plan (NCIRP) in collaboration with the private sector and other key stakeholders. The NCIRP provides a framework for effective incident response capabilities and coordination to ensure that all cybersecurity partners—including federal agencies, state and local governments, the private sector and international partners—are prepared to participate in a coordinated and managed response to a cyber incident.

3. Third, and the focus of my testimony today, is our efforts to increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

As you know, the term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as electricity, drinking water, and manufacturing. Control systems security is particularly important because of the inherent interconnectedness of the critical infrastructures and key resources (CIKR) sectors (i.e., water and wastewater treatment depends on the energy and chemical sectors, energy fuels transportation, and other sectors, etc.). We also rely on control systems to operate our federal, state, local, and tribal governments; therefore, assessing risk and effectively securing industrial control systems are vital to maintaining our nation's strategic interests, public safety, and economic well-being.

Cybersecurity – Critical Infrastructure Protection

Our nation depends on the continuous and reliable performance of a vast and interconnected critical infrastructure to sustain our way of life. Although each of the critical infrastructure industries, from energy though water treatment, is vastly different, they all have one thing in common: they are dependent on control systems to monitor, control, and safeguard their processes.

A successful cyber attack on a control system could potentially result in physical damage, loss of life, and cascading effects that could disrupt services. As such, DHS recognizes that the protection and security of control systems is essential to the nation's overarching security and economy.

In May 2004, the Department established the Control Systems Security Program (CSSP) to guide a cohesive effort between government and industry to reduce the cyber risk to industrial control systems. As part of this effort, the CSSP works to protect critical infrastructure by providing expertise, tools, and leadership to the owners and operators of control systems. The CSSP also leads development and implementation of the Department's *Strategy to Secure Control Systems* (Strategy).

Strategy to Secure Control Systems

The strategy helps to guide efforts—both public and private—to improve control systems security in the nation's critical infrastructure. The primary goal of the strategy is to build a long-term common vision for effective risk management of Industrial Control Systems (ICS) security through successful coordination of efforts among public and private stakeholders. The strategy identifies CSSP as the lead in evaluating cyber risk and serving as the focal point for coordinating cybersecurity activities, including risk management and incident response, for critical infrastructure asset owners and operators.

Risk Management

The CSSP conducts operational cyber risk management activities and strategic readiness initiatives to manage cyber risk. The Industrial Control Systems Computer Emergency Response Team (ICS-CERT) is the operational arm of CSSP, acting as the focal point for analyzing and coordinating response to incidents and threats impacting industrial control systems. The ICS-CERT works in coordination with the United States Computer Emergency Readiness Team (US-CERT) and is a component of the NCCIC. With regard to strategic readiness, CSSP has a number of program areas focused on cyber preparedness and risk management, including conducting training classes, providing input to standards development, producing informational cybersecurity products and tools, conducting onsite cybersecurity assessments, and overseeing the Industrial Control Systems Joint Working Group.

In partnership with the Department of Energy, which is the Sector Specific Agency responsible for the Energy Sector under the National Infrastructure Protection Plan, the Industrial Control Systems Joint Working Group provides a vehicle for stakeholders to communicate and partner across all critical infrastructure sectors to better secure industrial control systems. The Working Group is a representative group comprised of owners and operators, international stakeholders, government, academia, system integrators, and the vendor community. The purpose of the Working Group is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, deployment and secure operations of industrial control systems.

As you are aware, cybersecurity training is essential to increasing awareness of threats and the ability to combat them. To that end, CSSP conducts multi-tiered training through web-based and instructor-led classes across the country. In addition, a week-long training course is conducted at CSSP's state-of-the-art advanced training facility at the Idaho National Laboratory to provide hands-on instruction and demonstration. This training course includes a "red team/blue team" exercise in which the blue team attempts to defend a functional mockup control system, while the red team attempts to penetrate the network and disrupt operations. The positive response to this week-long course has been overwhelming, and the classes are filled within a few days of announcement. To date, more than 16,000 professionals have participated in some form of CSSP training through classroom venues and web-based instruction.

CSSP also provides leadership and guidance on efforts related to the development of cybersecurity standards for industrial control systems. CSSP uses these industry standards in a variety of products and tools to achieve its mission.

First, CSSP uses and promotes the requirements of multiple federal, commercial and international standards in its Cyber Security Evaluation Tool (CSET) which has been requested by and distributed to hundreds of asset owners. Tool users are evaluated against these standards based on answers to a series of standard-specific questions. CSET is also used by CSSP assessment teams to train and bolster an asset owner's control system and cybersecurity posture in onsite assessments. In fiscal year 2010, the program conducted more than 50 onsite assessments in 15 different states and two U.S. territories, including several remote locations where the control systems represent potential single points of failure for the community. The program is planning for 75 onsite assessments in fiscal year 2011.

Second, the program developed the *Catalog of Control Systems Security: Recommendations for Standards Developers*, which brings together pertinent elements from the most comprehensive and current standards related to control systems. This tool is designed as a "superset" of control systems cybersecurity requirements and is available in the CSET and on the website for standards developers and asset owners.

Lastly, the CSSP provides resources, including time and expertise, to standards development organizations including National Institute of Standards and Technology (NIST), the International Society of Automation, and the American Public Transportation

Association. Experts provide content, participate in topic discussions, and review text being considered by the standards body.

As a member of the Smart Grid Interoperability Panel, CSSP participated in the NIST Cybersecurity Working Group, which extensively used the CSSP-developed *Catalog of Control Systems Security: Recommendations for Standards Developers* to create a framework for assessing and mitigating risk to Smart Grid technologies in NIST Report 7628, *Guidelines for Smart Grid Cyber Security*.

In addition to performing assessments and participating in standards development, the CSSP has also created a series of recommended practices and informational products to assist owners and operators in improving the security of their control systems. These information resources are publicly available online[1] and are also promoted through the Working Group and other sector forums.

Incident Response

While these strategic readiness activities help to reduce overall risk to control systems, the industry needed an operational response group to turn to when actual cyber incidents occurred. In 2009, the CSSP established the Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) to coordinate response to and analyze control systems-related incidents, conduct analyses of vulnerabilities and malicious software, and disseminate cybersecurity alerts and advisories to all sectors. The ICS-CERT provides a focused operational capability to provide owners and operators of control systems situational awareness and technical assistance in the event of an incident. The ICS-

[1] http://www.us-cert.gov/control_systems/

CERT, in coordination with US-CERT, also provides onsite incident response to organizations that require assistance in responding to a control systems attack. For larger scale cyber attacks and generally, ICS-CERT coordinates with the other NCCIC components including US-CERT, the National Communications Center, and DHS Intelligence and Analysis to ensure appropriate levels of awareness and technical support.

Upon notification of an incident, the ICS-CERT performs a preliminary diagnosis to determine the extent of the compromise. At the impacted organization's request, ICS-CERT can deploy a fly-away team to meet on-site with the company or organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow-on analysis. ICS-CERT provides mitigation strategies and assists asset owners and operators in restoring service, as well as recommendations for improving overall network and control systems security. In fiscal year 2010, ICS-CERT conducted 13 incident response activities to organizations in need. During these assist visits, infected systems were identified and sanitized, and steady state operations were restored. In all cases, ICS-CERT assisted the organizations in developing focused mitigation plans, and provided access to tools for follow-on defensive measures. The increasing call for support and value-add that the organization has demonstrated has led to the need to augment ICS-CERT's force, which we plan to do in fiscal year 2011.

Coordination and Integration

The ICS-CERT coordinates control systems-related security incidents and information sharing with federal, state, and local agencies and organizations, as well as private sector constituents including vendors, owners and operators, and international and private sector computer emergency response teams.

In addition, the ICS-CERT leverages relationships with many working groups – including the Industrial Control Systems Joint Working Group and the Federal Control Systems Security Working Group – to increase and improve information sharing with critical infrastructure asset owners and operators and vendor community. It is through these relationships that private sector partners and vendors have called on the ICS-CERT during control systems emergencies and events.

In 2007, the CSSP studied several scenarios to evaluate the impacts of a successful cyber attack on critical control systems infrastructure in several critical infrastructure sectors, including energy and transportation. The studies used hypothetical, but credible, cyber attack scenarios that employed common hacking methods and knowledge of control systems. Consequences of the attacks ranged from multiple-day shutdowns of facilities without death or injury, to extensive system damages, casualties, and billions in economic loss. The scenario development took advantage of open source literature, in-house and industry cyber experts, CSSP research and documentation, and engineering analysis to assess the feasibility of a cyber attack and derive the outcomes with assessed damage. Additional scenario development and analysis was conducted for cyber attacks on a nuclear power generation plant, an electricity-generating station, and a large industrial facility. This analysis also yielded estimated consequences resulting in significant economic impact, major disruption to services, injuries and potential loss of life.

Stuxnet

While scenario analysis plays an important part of understanding and reducing risk to critical infrastructure, a real-world threat emerged earlier this year that significantly changed the landscape of targeted cyber attacks. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware. What makes Stuxnet unique is that it uses a variety of previously seen individual cyber attack techniques, tactics, and procedures, automates them, and hides its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring. The concern for the future of Stuxnet is that the underlying code could be adapted to target a broader range of control systems in any number of critical infrastructure sectors.

The ICS-CERT immediately began to analyze the code and coordinate actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers.

Our analysis quickly uncovered that this sophisticated malware has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. The malware is highly complex and contains over 4,000 functions, comparable to the amount of code in some commercial software applications.

Leveraging the unique capabilities and partnership with the Idaho National Laboratory, ICS-CERT was able to conduct sophisticated analysis on Stuxnet. ICS-CERT has documented that the malware was written to look specifically for computers running the Siemens WinCC Human Machine Interface (HMI). It then copies components into the associated Structured Query Language (SQL) database and checks to see if the HMI is connected to certain Siemens Simatic Programmable Logic Controller (PLC) models. If it finds the specific model of PLC, Stuxnet then checks for specific program elements in the PLCs and, if found, attempts to install rogue ladder logic into the PLC program.

ICS-CERT analysis indicates that the logic is only changed when these specific conditions are met. This selective infection criterion, along with the analysis of the logic injected by Stuxnet, indicates that a specific process was likely targeted. However, while we do not know which process was the intended target—it is important to note that the combination of Windows operating software and Siemens hardware can be used in control systems across critical infrastructure sectors—from automobile assembly lines to mixing baby formula to processing chemicals.

Furthermore, ICS-CERT concluded that Stuxnet was professionally created using carefully planned development concepts. The malware implements state-of-the-art techniques and capabilities for infecting a system, preventing detection (to maintain its presence), exfiltrating data, and inhibiting analysis once the code is detected. In other words, this code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product, and indicate to the operator and your anti-virus software that everything is functioning as expected.

To combat this threat, the ICS-CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July. To date, the ICS-CERT has briefed dozens of government and industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit.

Looking ahead, the Department is concerned that attackers could use the publicly available information about the code to develop variants targeted at broader installations of programmable equipment in control systems. The ICS-CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, on-site incident response activities, and information sharing and partnerships. The salient lesson of Stuxnet, and other emerging threats, is that the CSSP mission and coordination between DHS and the control systems community are vital to our efforts to protect the nation's critical infrastructure.

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, let me end by thanking you for the strong support you have provided the Department. Thank you for again for this opportunity to testify. I would be happy to answer your questions.

TESTIMONY OF MICHAEL J. ASSANTE

PRESIDENT AND CHIEF EXECUTIVE OFFICER
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS OF THE UNITED STATES INC.

**BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**

U.S. SENATE

Hearing on

SECURING CRITICAL INFRASTRUCTURE IN THE AGE OF STUXNET

November 17, 2010

Testimony of Michael J. Assante
National Board of Information Security Examiners
November 17, 2010

Good morning, Chairman Lieberman, Senator Collins, and members of the Committee. I am pleased to appear here this morning to testify on securing critical infrastructure in the age of Stuxnet.

My name is Michael Assante and I am the Chief Executive Officer of the National Board of Information Security Examiners ("NBISE"). NBISE is a newly-created, not-for-profit, certification body comprised of dedicated staff and a board of experts in information security practice and policy. NBISE is developing assessments, examinations, and certifications designed to uphold the highest standards of professionalism and practice in essential information security disciplines. I am here in this capacity and as someone who has worked in the field of critical infrastructure protection with a focus on industrial control systems security. I have served in the U.S. Navy, been responsible for both physical and cyber security of one of the largest electric utilities in the United States and worked on control system security research at the Idaho National Laboratory. I also recently held the position of the Chief Security Officer at the North American Electric Reliability Corporation ("NERC"), which serves as the Electric Reliability Organization ("ERO") in the United States and much of Canada.

I am pleased that this hearing has been convened to explore the implications of advanced cyber threats on the security of our nation and its critical infrastructure, as exemplified recently by the Stuxnet worm. The Stuxnet code is a worthy centerpiece for this discussion, but I believe this is neither the first nor the last attempt to compromise and use operational systems to effect physical outcomes. Stuxnet is, at the very least an important wake up call for digitally-enhanced and reliant countries; and at its worst, a blueprint for future attackers.

There are many lessons that we must learn from this particularly sophisticated piece of malicious code. Because it will set the course for cyber strategy and policy, our response to this demonstration of the new cyber reality is critical. Developing and implementing effective indicators, defenses, and countermeasures to cyber threats like Stuxnet demands that we look not just to the security community but also to the system designers, planners, engineers, and operators of our essential technology and physical infrastructures. We must take a prudent and proactive approach that enhances our ability to learn and apply knowledge fast enough to manage the dangerous consequences that come with these types of attacks. We can no longer ignore known system weaknesses and simply accept current system limitations. We must admit that our current security strategies are too disjointed and are often, in unintended ways, working against our efforts address the highly-advanced security challenges facing our cyber-dependent critical infrastructures.

My statement will paint a very difficult challenge, but it is important to note that I remain an optimist about our ability to close the gap. This nation, as it has done in countless past contests, should turn to its men and women, in and out of uniform, to muster an effective defense. Our obligation is to effectively organize, train, and equip them to be successful in this important task.

Testimony of Michael J. Assante
National Board of Information Security Examiners
November 17, 2010

THE DISRUPTIVE INNOVATION THAT IS STUXNET

Simply put, Pandora's Box was opened years ago as the United States became reliant upon digital technology to help operators control complex processes. Stuxnet is an important harbinger of things that may come if we do not use this opportunity to learn about this threat (and others like it) to our infrastructure control systems. No one should be shocked that cyber exploits can be engineered to successfully compromise and impact control systems. Study after study has identified common vulnerabilities found across control system products and implementations. The exploitation of a hard-coded password design in one vendor's implementation will not be an uncommon or isolated occurrence.

Stuxnet is a good example of a cyber threat that was thought to be hypothetically possible, but not considered probable by many. Its features, capabilities, and intended technology target/purpose should disturb security professionals, engineers, businessmen, and government leaders alike. There are three specific reasons why I make this important statement:

First, it appears there is a group of well-resourced people possessing the necessary motivation, who have successfully acquired the knowledge, skills, and capabilities to systematicall develop and launch a highly-sophisticated attack targeting control systems to effect a desired physical outcome. The public occurrence of such a cyber attack is important as it dispels conventional thinking that it is just "too hard" for an attacker to assemble the necessary information, gain familiarity with the technology, acquire the knowledge of specific implementations, configurations and accesses to devise an attack that could disrupt or damage the physical components of an industrial process. It requires more resources and skill, by a cyber attacker, to attack control systems with sufficient confidence to achieve a specific and intended outcome. The authors of Stuxnet have certainly established themselves in this category. I am, however, concerned that an attacker with less means might still be capable of creating havoc or unintentionally causing a more isolated accident.

What is shocking to control system security experts is not that it was done, but that it was done in such a manner as to rely upon pre-programmed code that had the ability to autonomously analyze the system that had been compromised and identify the specific conditions desired for the delivery of its "digital warhead." Most had anticipated more manual attacks capable of achieving negative consequences to physical process, through a more stepped process of compromise, discovery, learning, and action.

The authors of Stuxnet were able to characterize the environments that it would compromise and develop enough capability and logic to defeat anticipated security measures, deal with different configurations, practices and architectures, and act in a very restrained manner until it found its ultimate target. The lesson that we must not gloss over is that highly resourced actors can assemble people capable of planning on how to deal with system variances, security controls, obscure and proprietary technology, and complex industrial processes.

This complex and sophisticated code had been propagating for months before it was identified and recognized as something different. Security researchers inspecting the code soon discovered a code base that was professionally developed and tested. This threat was wrapped in layers of obfuscation like many pieces of custom malicious code, but a closer inspection revealed advanced techniques for circumventing a number of anticipated security controls to include signature-based security tools, behavior-based detection engines and the requirement for files signed with certificates. The authors took advantage of combining known vulnerabilities with a never before seen use of four "zero-day" (or previously unknown) exploits to compromise systems. This allowed the code to escalate privileges, embed itself, propagate further, receive updates, and seek out its intended target. It is not beneficial to speculate on the worm's ultimate target, but I was relieved to hear that it was programmed to inject code only when specific configurations and processes were identified. It is difficult to imagine what would have happened if the authors were interested in creating more general havoc and had programmed the worm to be less constrained in injecting changes to victim controllers.

Second, we must understand that the attacks we should be most concerned with are not designed to disable their digital targets, but to manipulate them in an unintended way to achieve a desired physical outcome. Many professionals have limited their thinking to dealing with the loss of individual elements or capabilities of their control systems and have failed to fully embrace the implications of calculated misuse. I attempted to shed light on this important topic in my April 7, 2009 letter to the electricity industry (also submitted for the record).

The ability of an attacker to access controllers, safety systems, and protection devices and inject valid or malicious code that can change set points, command action, change the expected logic, or suppress a measurement and/or action is alarming. I have participated in research that demonstrated this capability in a controlled environment to understand how it could be done and explore the potential consequences should such a weapon materialize. I believe that the analysis to date has indicated that Stuxnet may be such a weapon. To complicate matters, we have not sufficiently studied nor considered the potential for these types of attacks on large interconnected systems such as the electric grids or in highly controlled and potentially dangerous industrial processes.

We must not put our faith in the possibility that the necessary knowledge of these types of attacks will remain only in the hands of highly-educated and trained process control engineers. The first, generally accepted, industrial control system ("ICS") vulnerability was disclosed to the public in 2005. As of October 1, 2010, the national vulnerability database has 51 vulnerabilities currently listed, and organizations like Critical Intelligence are tracking 119 disclosed vulnerabilities. A dedicated attacker, even without first-hand, detailed knowledge of how to program and apply control system technology can still cause serious damage. I have worked with general cyber security researchers that have developed capabilities to compromise and affect industrial control systems. One can develop such capabilities by accessing production systems, acquiring and experimenting with components, and gathering technical information available on the web. The researchers demonstrated that gaining access to control system data streams, systems, and specific devices can be enough to attack the process being controlled or safeguarded. For example, in modern control systems most of the process safety depends on logic found in the controllers. By analyzing this code one can not only determine what the engineer wants to happen but also what the engineer wants to avoid. One can identify how to cause negative effects by studying the programmed logic, like master-stop conditions, to identify ways to achieve unsafe conditions or override safety shutdown logic.

It is critical that we reverse many of the trends in the control and safety system market that make an attacker's task of causing damage in the physical world easier. One such trend is the convergence of control systems and safety systems at the network-level. An all-too-familiar tale has us achieving greater efficiencies by doing away with silos and leveraging shared network resources. Legacy industrial systems relied on physically separate and functionally independent control and safety systems. The safety system could independently sense and act to ensure the safety or reliability of the system/process. Today, we see an alarming trend towards sharing network resources in space and cost-constrained industrial applications so that the safety system is now only functionally and logically separated from the control system. This dangerous trend provides far too great an opportunity to an attacker in high-consequence environments, enabling access to both safety and control systems from a single point of entry. This is significant as an attacker can explore and manipulate the safety system; removing planned safeguards, before misusing the control system to create a dangerous condition.

Finally, our current defense and protection models are not sufficient against highly-structured and resourced cyber adversaries capable of employing new and high-consequence attacks. Our defensive thinking has been shaped by the more frequent and more survivable threats of the past. As a result of this paradigm, our security architectures and security market solutions are mostly reactive by nature. This is a logical behavior because the market and security organizations primarily respond to attacks that have been observed in sufficient numbers to warrant the development of countermeasures and new practices. This behavior is less risky in applications that adhere to the restrictions of scale, time and geographic space. An example of this is the realm of physical security, where the capabilities of attackers typically evolve at a slower pace and an attacker is often constrained when using a new capability in a fashion that is limited by both time and their ability to be physically present in a single location. Computers and networks provide for less constrained circumstances and the ability to develop new attack techniques and tactics evolve very rapidly and change with the very technology it attacks. One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from anywhere, and without fear of attribution.

This means that while current cyber defense tactics, security architectures and tools are necessary and can be responsive to the most likely of threats, they are not sufficient to deal with new advanced threats. The optimist always points to a new type of security tool or practice as the solution to current protection inadequacies. I have watched the industrial system and security community rush towards the technology of white-listing as an answer to the Stuxnet worm. This technique can be effective and is an important option to deploy, but we should not believe that if it had been necessary to assure their success, the authors of the Stuxnet worm would not have simply developed a way to counter this measure. In support of this assertion, the experts at Symantec studied the capability of this worm and concluded that the authors had the resources necessary to counter anticipated market-produced security solutions.

I appreciate the strong desire to create reactive solutions but I believe that desire leads to tunnel vision limiting our approach to prevention and detection strategies. It is important that we do not place our faith solely in conventional security tactics and tools. The shortfalls of our current tools are becoming apparent to many specialists desperately working to clean up the Stuxnet infections. They have reported great difficulty in removing the problem. Many of the security research programs funded by the government are working to research and implement yesterday's general information technology (IT) security measures into today's operational ICS and Supervisory Control and Data Acquisition ("SCADA") systems. These efforts were proven ineffective in general IT systems against more advanced threats and don't represent a wise use of our resources. They will not significantly improve the safety and reliability of our physical infrastructures against well-resourced attackers. In short, we are preparing for the next battle by using pre-2003 strategies and weapons.

THE SUSCEPTIBILITY OF OUR CRITICAL INFRASTRUCTURE

I would like to provide some additional perspective by focusing on the electricity infrastructure because I am experienced with its operations and protection challenges. I would like to begin by prefacing my comments with an observation about the electric utility industry. I have seen this industry express a genuine desire to put system reliability first and can appreciate the unique pride that comes with serving communities with such an essential service. Cyber and physical security are two of many reliability risks faced by power system planners and operators. It is important to note that there are also various High Impact Low Frequency threats to consider. While the industry deals with some physical security events like copper theft on a regular basis, other more complex physical and technical threats or hazards, such as terrorism, electromagnetic pulse and space weather, are concerns as well and will require careful consideration to develop appropriate and effective mitigation.

Cyber-related threats pose a special set of concerns because they can arise virtually anytime, anywhere and change without warning. Unlike other operational and reliability concerns, such as extreme weather or the probabilistic failure of mechanical equipment, cyber-related events and threats could occur through accidents or by actors who intentionally manipulate or disrupt normal operations as part of a premeditated design to cause damage.

The susceptibility of our modern interconnected and digitally reliant infrastructures is well established. We must now find answers to research and engineering challenges associated with protecting those infrastructures for which significant damage, and the lack of availability for extended periods of time, would have catastrophic impacts on society. Efforts to modernize our nation's electric power infrastructure through the overlay of two-way digital communications and highly-automated digital control (to create the "smart grid") are based on the desirable promise of greater energy efficiency and system performance. Of course, more technology typically adds more complexity and interconnectedness. We should continue to seek progress, but also recognize the need to close the gaps in the software and system engineering foundations necessary to ensure that new smart grid functionality will be secure, safe, survivable, reliable, and resilient.

The most fundamental of these research and engineering challenges is how to design, configure, and operate the smart grid's systems and components in a manner that prevents an adverse cyber-physical event (whether accidental or malicious in origin) from having a catastrophic impact on the grid and on society at large. For examples of the kinds of adverse events, see the "Coordinated Attack Risk" chapter of the recent joint report by NERC and the U.S. Department of Energy ("DOE"), entitled *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*[1].

REGULATING CYBER SECURITY & NERC'S MANDATORY RELIABILITY STANDARDS

NERC-developed critical infrastructure protection ("CIP") Reliability Standards represent an early attempt to manage cyber security risks through mandatory standards with significant penalties for non-compliance. It is clear to me that the standards as written and implemented are not materially contributing to the management of risk posed by advanced cyber threats, such as the Stuxnet worm.

The standards are comprised of forty-three specific requirements designed to provide a minimum set of sound security practices that, if properly implemented, can serve as a simple foundation to be built upon. The perimeter protection model taken by the standards is more aligned with cyber threats of yesterday and is most effective against less structured types of cyber attacks. The standards also include significant gaps and exclusions, but their greatest weakness is in how they have been implemented. These standards have polarized the industry and have imposed requirements on a highly-dynamic and not fully understood area of system risk. The result has been a conscious and inevitable retreat to a compliance/checklist-focused approach to the security of the bulk power system. I have observed security programs that have suffered from resources being channeled into compliance activities and a hesitance, or even outright refusal to try ideas, measures, and security practices that exceed what is called for in the standards. Unfortunately the NERC CIP Standards have become a glass ceiling for many utility security programs, which prevents the emergence of the type of security programs we need to deal with Stuxnet-like attacks.

I believe the level of expertise needed to create standards that achieve security objectives and ensure safety and reliability must be found not in one quarter, such as within industry or a specific government agency, but within the community at large. There must be a process that will maximize the contributions from security, industry, and technology experts, while establishing a mechanism to identify the best performance measures to manage the risk. At this point it seems clear that saying "industry knows best" about what is important enough to deserve enhanced protections and how best accomplish mitigation of advanced cyber risks is not completely accurate. We are all amateurs in this quest. I have first-hand experience working with mandatory standards. It is clear to me that standards are a good tool to manage risk when it is either well-bounded and understood or when the standard simply codifies well-honed industry practices that are proven to be successful. Mandatory cyber standards fail both of these conditions, mainly because advanced cyber threats are not probabilistic in nature, but represent a

[1] Available at: http://www.nerc.com/files/HILF.pdf

co-adaptive risk. The best decisions will only come from an active engagement of experts in and out of government, industry, and the larger community under strong leadership.

Regulation, although necessary, should be re-evaluated and designed to emphasize learning, enable the development of greater technical capabilities through more qualified staff, and discourage the creation of a predictable and static defense. For example, both asset owners and technology vendors must be prepared to recognize and be required to report significant and unique security incidents to key stakeholders, including peer organizations. The requirement to report cyber incidents should be accompanied by a fair and limited safe harbor to promote this essential requirement (consider the model established by FAA and NASA regarding commercial pilot event reporting). Informed regulatory oversight will be necessary to shepherd the process so it is capable of producing timely results without harming the very systems we are trying to protect.

A joint rule-making arrangement between an office responsible for coordinating regulation across the critical infrastructure sectors and a more directly aligned government agency or independent commission is best suited for this leadership task. I believe that more clearly defined federal authority and funding is needed to address specific and imminent cyber security threats to critical infrastructure. If we were discussing the electricity sector the coordination authority would need to work jointly with FERC, as they better understand the reliability issues associated with the technology and operations of the sector. Again in the case of the power system, this effort will need to be closely coordinated with Canada as oir physical infrastructure is critically tied to that of our northern neighbor. Ultimately we will have to require security concerns to be factored into design choices and architectures, not just addressed by technical system security standards.

IMPLICATIONS

Cyber threats will continue to evolve and the extent of their potential to negatively impact our control systems is not yet fully appreciated. The potential for an intelligent attacker to exploit a common vulnerability that impacts many assets at once, and from a distance, is one of the most concerning aspects of this challenge. This is not unique to the electric sector. Addressing it, however, will require asset owners to apply additional, new thinking on top of sound operating and planning analysis when considering appropriate protections against these types of threats. It is imperative as a nation that we seek to broaden the understanding of cyber risk concerns facing the interconnected networks and critical infrastructure. We must develop and implement protection strategies that accept the unfortunate, though probable, reality that many of our networks are already contested territory. Accepting this important assumption will help stimulate industry and community efforts to develop new and prudent approaches to address the most material risks.

In the realm of cyber, we must recognize the potential for simultaneous loss of assets and common modal failure in identifying what needs to be protected or engineered to be more survivable. This requires a shift of our priorities from a prevention-heavy approach to reduce the likelihood of such an event from occurring to a greater focus on minimizing the possible consequences of such an event. We must tackle these types of threats by investing in the development of our security professionals, engineers, and operators, and establish countermeasures and mitigations in a far more comprehensive manner. This requires us to consider not only security, but also how we can design and engineer survivability into our complex systems, achieve resilience in our organizations, technology and process, and better prepare to respond and recover.

A significant cause for concern is that much of the information about cyber-security-related threats remains classified in the homeland security, defense and intelligence communities, with restricted opportunity to share information with security researchers, technology providers and affected private-sector asset owners. Our nation's critical infrastructure is placed at significant risk as a result of limited progress to support learning and the application of newly gained knowledge to protect or even respond to and recover from advanced cyber threats.

A mechanism is needed to quickly validate the existence of advanced threats and to ensure information is appropriately conveyed to and understood by asset owners and operators in order to mitigate or avert cyber vulnerabilities. A complex cyber threat cannot be easily contained and has the potential to undermine the integrity of systems owned by governments and private sector organizations alike. We must develop a better framework for tapping into the best and brightest, whether they are specialists holding clearances in the federal government, professionals conducting cutting-edge research into security problems (for example, Symantec engineers and ICS security specialists), those on the ground managing ICS, or others developing and providing technology, or managing complex control system environments. Efforts should be taken to develop standing and situation-based pools of expertise to quickly analyze specific threats and develop guidance to respond, mitigate and if possible, protect critical systems. Critical infrastructure organizations need to develop the ability to identify information relevant to the risks they face and work with the broader national security community to better understand adversary intent, capability (tactics, techniques and procedures both demonstrated and assessed) and opportunity to effectively prioritize and structure countermeasures and mitigations. Government agencies, asset owners, technology providers and researchers have clung to our different identities for too long. Having a common mission is not enough we need to develop the policies, practices, and tools to operate in a unified manner, much like coalition military operations. We need to raise both our individual and collective community capabilities to address these sophisticated and dangerous threats.

I would like to specifically emphasize one of the necessary investments to combat advanced cyber threats like Stuxnet. Though the size, configuration, and function of information networks can vary widely, there is a single feature common to each of them: behind every firewall, system architecture, and vulnerability assessment stands an information security professional. Through the years, working as a Chief Security Officer at a major utility, or supporting researchers, coordinating protection efforts while at NERC, I have gained an appreciation for the importance and the difference made by skilled and well-developed people. I have never understood why we have not embraced better training and development methods for our frontline security and operations staff. We train pilots using advanced simulators to deal with difficult conditions and mechanical failures. Why do we not use simulators to allow security and operational staff to experience low frequency but high consequence attacks against the systems they defend and operate? Why do we not use performance-based examinations to qualify our most important resources? We have allowed chance to be our school house, where targeted organizations simply suffer in silence, not willing to pass along the tough lessons they have learned to others.

Effective security and response against highly advanced cyber threats requires a current understanding of what adversaries are capable of, an opportunity to experience directed attacks to become familiar with observables and experiment with response actions, and the use of a team training framework to optimize defender tactics, techniques and procedures. We must embrace virtual gaming technology and look for ways to stimulate defensive technology with simulated attacks so what has traditionally been only a hypothetical or has been overlooked can made real for the purposes of learning and preparing. It is time that we more formally prepare these individuals and ensure they are competent, prepared, and capable of making the right decisions day-to-day and during emergencies.

CONCLUSION

I commend this Committee for its exploration of the implications that advanced threats like Stuxnet pose to our critical infrastructure and nation. I look forward to supporting your efforts in any way possible. Stuxnet should cause all of us to re-think how we are prepared to protect, respond, and survive future cyber challenges to operational technology like control, safety and protection systems. We must be better prepared to learn about our weaknesses; identify and understand new threats; and make better design, deployment, and operations decisions. We must waste no more time in debating our susceptibility. We must accept that well-resourced adversaries are currently able to achieve primacy by developing unique and creative tools to compromise and affect control system technology. These adversaries may also be capable of causing damage to industrial processes in difficult to anticipate ways. It is time to turn our attention to addressing known weaknesses, researching consequences, designing our security, training and preparing our operations staffs and finding ways to make our systems more resilient. The following steps are necessary:

- Remove and remediate architectural weaknesses, known vulnerabilities, and poor security designs in industrial control systems.

- Promote greater progress designing and integrating security/forensic tools into control environments. But, put your faith and focus in people not the tools of the day.

- Prioritize our efforts by jointly studying the potential consequences that may result from directed and well resourced attacks of control, safety and protection systems in high risk segments of the critical infrastructure. In the cases where the consequences are unacceptable we must assume the attacker can successfully defeat our security and therefore direct our efforts to engineering away that risk with more survivable designs and practices.

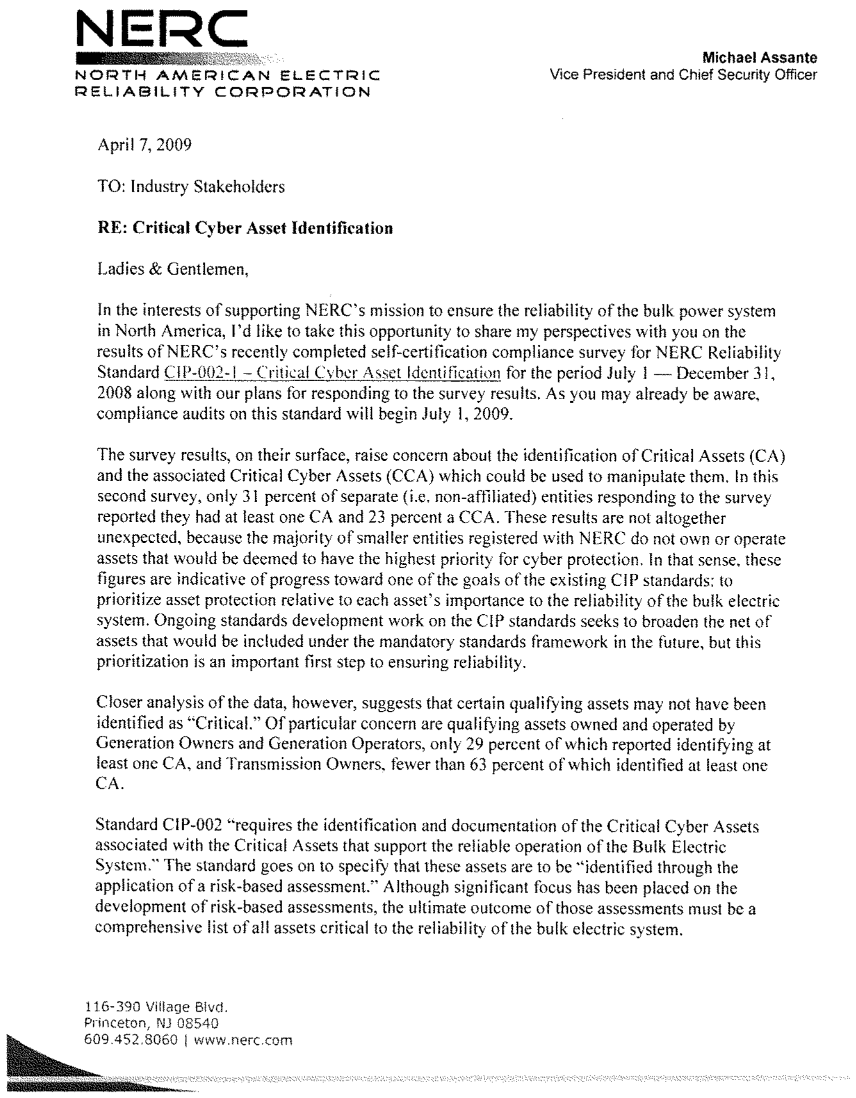
- Organize a well-funded, multi-year research & development program to design toward a more resilient infrastructure. The research should include safety system design; explore dedicated networks; architecting complex systems to severe system optimization and preserve core system functions, when needed.

- Establish new regulation in the form of risk-based performance requirements that value learning, promote innovation, and better equip/prepare control environments and the teams that protect, operate, and maintain them. The current regulatory structure will not, in my view, be capable of achieving this end. Legislation should include the need for more sharply defined federal authority to address specific and imminent cyber security threats to critical infrastructures in the form of emergency measures.

- Require critical infrastructure asset owners and control system vendors to report industrial control system specific security incidents and the U.S. government must provide up-to-date information to asset owners and operators on observed adversary tactics and techniques, especially when investigations reveal attacker capabilities to side-step or exploit relied upon security technologies.

- Invest in the workforce that defends and operates our infrastructure systems. Scalable immersive training environments and local simulator/stimulator training technology should be used to optimize the development of defender skills. The same workforce should then be qualified through periodic rigorous performance-based assessments and, where appropriate, examinations.

My greatest fear is that we are running out of time to learn our lessons. Stuxnet, although difficult to hijack or modify by others, may very well serve as a blueprint for similar but new attacks on control system technology. We know that ordinary high-risk practices, such as the use of USB sticks by plant personnel and contractors, must be modified. We know that well-known security weaknesses in ubiquitous technologies need to be re-evaluated and protected. We know that addressing security at the network and general IT layer only addresses one of many attack paths and we must start addressing the exploitable weaknesses of field control devices (such as Remote Terminal Units, Programmable Logic Controllers, and other Intelligent Electronic Devices). Ultimately, we know that our conventional approach to more common security threats will be necessary but woefully insufficient to protect these systems from the next Stuxnet-like cyber threat. We must act now to develop our greatest resource in this contest; the professionals that defend, operate, and protect our critical systems and infrastructure.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Michael Assante
Vice President and Chief Security Officer

April 7, 2009

TO: Industry Stakeholders

RE: Critical Cyber Asset Identification

Ladies & Gentlemen,

In the interests of supporting NERC's mission to ensure the reliability of the bulk power system in North America, I'd like to take this opportunity to share my perspectives with you on the results of NERC's recently completed self-certification compliance survey for NERC Reliability Standard CIP-002-1 – Critical Cyber Asset Identification for the period July 1 — December 31, 2008 along with our plans for responding to the survey results. As you may already be aware, compliance audits on this standard will begin July 1, 2009.

The survey results, on their surface, raise concern about the identification of Critical Assets (CA) and the associated Critical Cyber Assets (CCA) which could be used to manipulate them. In this second survey, only 31 percent of separate (i.e. non-affiliated) entities responding to the survey reported they had at least one CA and 23 percent a CCA. These results are not altogether unexpected, because the majority of smaller entities registered with NERC do not own or operate assets that would be deemed to have the highest priority for cyber protection. In that sense, these figures are indicative of progress toward one of the goals of the existing CIP standards: to prioritize asset protection relative to each asset's importance to the reliability of the bulk electric system. Ongoing standards development work on the CIP standards seeks to broaden the net of assets that would be included under the mandatory standards framework in the future, but this prioritization is an important first step to ensuring reliability.

Closer analysis of the data, however, suggests that certain qualifying assets may not have been identified as "Critical." Of particular concern are qualifying assets owned and operated by Generation Owners and Generation Operators, only 29 percent of which reported identifying at least one CA, and Transmission Owners, fewer than 63 percent of which identified at least one CA.

Standard CIP-002 "requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System." The standard goes on to specify that these assets are to be "identified through the application of a risk-based assessment." Although significant focus has been placed on the development of risk-based assessments, the ultimate outcome of those assessments must be a comprehensive list of all assets critical to the reliability of the bulk electric system.

A quick reference to NERC's glossary of terms defines a CA as those "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Most of us who have spent any amount of time in the industry understand that the bulk power system is designed and operated in such a way to withstand the most severe single contingency, and in some cases multiple contingencies, without incurring significant loss of customer load or risking system instability. This engineering construct works extremely well in the operation and planning of the system to deal with expected and random unexpected events. It also works, although to a lesser extent, in a physical security world. In this traditional paradigm, fewer assets may be considered "critical" to the reliability of the bulk electric system.

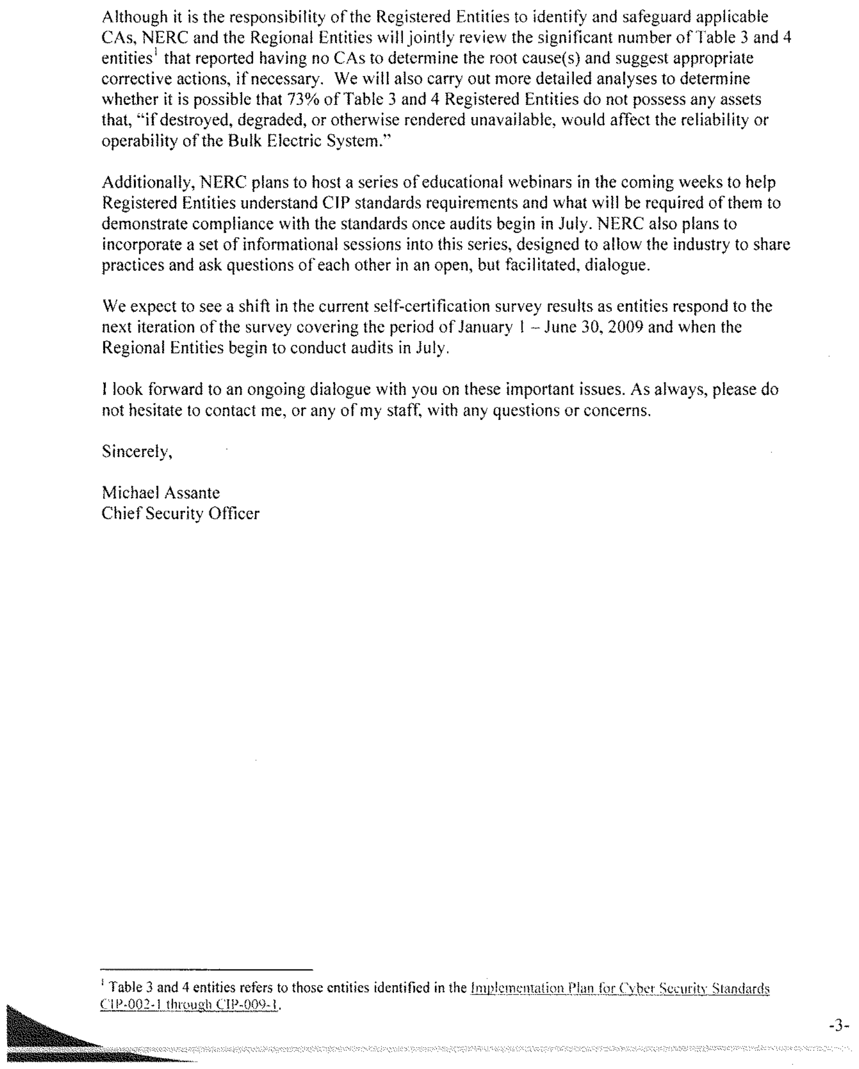
But as we consider cyber security, a host of new considerations arise. Rather than considering the unexpected failure of a digital protection and control device within a substation, for example, system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word "manipulate" here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new "cyber security" paradigm. A number of system disturbances, including those referenced in NERC's March 30 advisory on protection system single points of failure, have resulted from similar, non-cyber-related events in the past five years, clearly showing that this type of failure can significantly "affect the reliability (and) operability of the bulk electric system," sometimes over wide geographic areas.

Taking this one step further, we, as an industry, must also consider the effect that the loss of that substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it.

One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance. The majority of reliability risks that challenge the bulk power system today result in probabilistic failures that can be studied and accounted for in planning and operating assumptions. For cyber security, we must recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected. This is why protection planning requires additional, new thinking on top of sound operating and planning analysis.

"Identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System" necessitates a comprehensive review of these considerations. The data submitted to us through the survey suggests entities may not have taken such a comprehensive approach in all cases, and instead relied on an "add in" approach, starting with an assumption that no assets are critical. A "rule out" approach (assuming every asset is a CA until demonstrated otherwise) may be better suited to this identification process.

Accordingly, NERC is requesting that entities take a fresh, comprehensive look at their risk-based methodology and their resulting list of CAs with a broader perspective on the potential consequences to the entire interconnected system of not only the loss of assets that they own or control, but also the potential misuse of those assets by intelligent threat actors.



Although it is the responsibility of the Registered Entities to identify and safeguard applicable CAs, NERC and the Regional Entities will jointly review the significant number of Table 3 and 4 entities[1] that reported having no CAs to determine the root cause(s) and suggest appropriate corrective actions, if necessary. We will also carry out more detailed analyses to determine whether it is possible that 73% of Table 3 and 4 Registered Entities do not possess any assets that, "if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Additionally, NERC plans to host a series of educational webinars in the coming weeks to help Registered Entities understand CIP standards requirements and what will be required of them to demonstrate compliance with the standards once audits begin in July. NERC also plans to incorporate a set of informational sessions into this series, designed to allow the industry to share practices and ask questions of each other in an open, but facilitated, dialogue.

We expect to see a shift in the current self-certification survey results as entities respond to the next iteration of the survey covering the period of January 1 – June 30, 2009 and when the Regional Entities begin to conduct audits in July.

I look forward to an ongoing dialogue with you on these important issues. As always, please do not hesitate to contact me, or any of my staff, with any questions or concerns.

Sincerely,

Michael Assante
Chief Security Officer

[1] Table 3 and 4 entities refers to those entities identified in the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1.

Symantec.

Prepared Testimony and
Statement for the Record of

Dean Turner
Director, Global Intelligence Network,
Symantec Security Response
Symantec Corporation

Hearing on

Securing Critical Infrastructure in the Age of Stuxnet

Before the

United States Senate
Committee on Homeland Security
And Governmental Affairs

November 17, 2010
342 Dirksen Senate Office Building

INTRODUCTION

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the opportunity to appear here before you today to discuss the Stuxnet worm and the important topic of securing the industrial control systems that underpin our nation's critical infrastructure.

My name is Dean Turner and I am the Director of Symantec's Global Intelligence Network which is part of Symantec Technology and Security Response[1]. My primary responsibilities include managing Symantec's DeepSight[2] Analyst teams and security intelligence. I also co-author and manage Symantec's *Internet Security Threat Report* which is a trusted source of global research and analysis of cyber attack data gathered from our DeepSight Threat Management System, Managed Security Services, Business Intelligence Services and Antivirus Research Automation.

As the global information security leader, Symantec protects more people and businesses from more online threats than anyone in the world. Our best-in-class Global Intelligence Network[3] allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. In short, if there is a class of threat on the Internet, Symantec knows about it.

Critical infrastructure protection is a top priority at Symantec as we are committed to assuring the security, availability and integrity of our customers' information. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure these critical systems from cyber attack. In my testimony today, I will provide the Committee with:

- Symantec's latest assessment of the Stuxnet worm including an analysis of the threat that this malware poses to Industrial Control Systems;

[1] Symantec is a global leader in providing security; storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

[2] Symantec™ DeepSight™ Threat Management System provides actionable intelligence covering the complete threat lifecycle, from initial vulnerability to active attack. With personalized notification triggers and expert analysis, the system enables enterprises to prioritize IT resources in order to better protect critical information assets against a potential attack. Powered by the Symantec Global Intelligence Network, the service is an authoritative source of tailored information about known and emerging vulnerabilities, threats, risks and global attack activity.

[3] Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify, analyze, deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services as well as additional third-party data sources.

- Our Insights into the major challenges and vulnerabilities associated with better securing the critical infrastructure from cyber attacks in the future;
- Observations on how the public and private sector can better secure these systems; and
- Several policy recommendations for the Committee's consideration to enhance the nation's critical infrastructure preparedness and resilience.

THE STUXNET WORM

I begin my testimony today by providing Symantec's observations of the Stuxnet worm as well as offering some insights on the implications that this threat poses to the nation's industrial control systems. As the Committee is aware, Stuxnet is a Windows-specific computer threat first discovered in June 2010. It is the first threat that Symantec has identified that spies on and reprograms industrial control systems, and is also the first to include a programmable logic controller (PLC) rootkit and, the first to target critical industrial infrastructure. It was written specifically to attack Industrial Control Systems used to control and monitor industrial processes, and not only can it reprogram PLCs, but also it can hide the changes.

Stuxnet is an incredibly large and complex threat. In fact, it is one of the most complex threats that we have analyzed to date at Symantec. I would like to draw the Committee's attention to a recent Symantec research paper entitled, *W32.Stuxnet Dossier*[4], in which we provide a detailed examination of Stuxnet and its various components with a particular focus on analyzing the final goal of Stuxnet, which we believe is to reprogram industrial control systems.

Symantec examined each of the different components of Stuxnet in an effort to better understand how the threat works in detail while keeping in mind that the ultimate goal of the threat is the most interesting and relevant part of the threat. Stuxnet is a threat targeting a specific industrial control system, such as a gas pipeline or power plant. To date, the majority of infected systems appear to be in Iran. We speculate that the ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries, and to hide those changes from the operator of the equipment.

In order to achieve this goal, the creators of Stuxnet amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.

Industrial control systems are automated through special code contained in the PLCs—for instance, to operate and control machinery in a plant or a factory. Stuxnet can steal code and design projects and also hide itself using a classic Windows rootkit, but unfortunately it can also do much more. Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems. Stuxnet effectively hides certain programming code, so when a programmer using an infected machine tries to view all the code on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC.

[4] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," September 20, 2010, version 1.0, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

In particular, Stuxnet hooks the programming software, which means that when someone uses the software to view code blocks on the PLC, the injected blocks are nowhere to be found. This is done by hooking enumeration, read, and write functions so that you cannot accidentally overwrite the hidden blocks as well. Stuxnet contains 70 encrypted code blocks that appear to replace some "foundation routines" that take care of simple yet very common tasks, such as comparing file times and others that are custom code and data blocks. Before some of these blocks are uploaded to the PLC, they are customized depending on the PLC.

By writing code to the PLC, Stuxnet can potentially control or alter how the system operates. A previous historic example[5] includes a reported case of stolen code that impacted a pipeline. In this case, code was secretly "Trojanized" to function properly and only some time after installation it instructed the host system to increase the pipeline's pressure beyond its capacity. This resulted in a three kiloton explosion, about one-fifth the size of the Hiroshima bomb.

STUXNET'S THREAT TO ICS SYSTEM SECURITY

Stuxnet demonstrates the vulnerability of critical national infrastructure industrial control systems to attack through widely used computer programs and technology. Stuxnet is a wake-up call to critical infrastructure systems around the world. This is the first publicly known threat to target industrial control systems and grants hackers vital control of critical infrastructures such as power plants, dams and chemical facilities. Stuxnet also represents the first of many milestones in malicious code history – it is the first to: exploit four zero-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator -- all in one threat.

Whether Stuxnet will usher in a new generation of malicious code attacks towards real-world infrastructure—overshadowing the vast majority of current attacks affecting more virtual or individual assets—or if it is a once-in-a-decade occurrence remains to be seen. Stuxnet is of such great complexity—requiring significant resources to develop—that a select few attackers would be capable of producing a similar threat, to such an extent that we would not expect masses of threats of similar sophistication to suddenly appear. However, Stuxnet has highlighted that direct-attacks to control critical infrastructure are possible and not necessarily spy novel fictions. The real-world implications of Stuxnet are beyond any threat we have seen in the past. Symantec was able to reverse engineer Stuxnet in order to better understand its purpose.

The intended target of Stuxnet is not known. Short of finding out the exact hardware configuration of every ICS system in the world we cannot be sure of the true extent of Stuxnet's victims. Speculation pointing to Iran as the likely target is just that–speculation. The large number of Stuxnet infections in that country may merely be a consequence of other factors. It is unknown who exactly is behind the Stuxnet attack. We know even less about who could have written Stuxnet than the target itself. Portions of Stuxnet's code that suggest authorship are vague at best; there is nothing in the code that could be taken to be a definitive link to anyone. What we *do* know is that whoever was behind it had good knowledge of ICS systems, particularly those they targeted. In addition, using so many un-patched vulnerabilities in just one malware family is unheard of outside of Stuxnet, again suggesting that these authors are more sophisticated than the typical cybercriminalgangs or attackers.

Without better knowledge of the persons behind these attacks, it is nearly impossible to say with any certainty who was responsible and possible motives behind the attack. The combination of sophisticated attacker and

[5] Nicolas Falliere, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," August 10, 2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

target means that any guesses of who was behind this is nothing more than speculation. However, the implications of Stuxnet's ability to modify commands sent to SCADA systems are significant. Industrial control systems under SCADA control that were targeted by Stuxnet could be damaged or outright destroyed, depending on the modified commands sent.

PROTECTING ICS NETWORKS AGAINST STUXNET AND FROM SIMILAR THREATS

The first obvious measure to protecting ICS networks from Stuxnet and similar threats is to deploy an anti-malware solution, and assure it is kept up to date. Of course, many SCADA systems today need to be modernized in order to even be capable of receiving anti-malware solutions. A good place to start in modernizing an SCADA system is with incorporation of Web-based capabilities. The functionality standard in web-enabled HMI workstations today significantly surpasses those of only a few years ago. Newer units can be configured to perform sophisticated notification of incidents and to respond automatically with cellular text messages, email or autodial phone calls. Such can simplify remote location monitoring and allow operators to respond to threats in a quicker fashion.

However, anti-malware alone does not provision the entire security landscape. The second most important element is to watch out for vendor security notifications and alerts, and to apply patches or workarounds as soon as possible. Next, ensure that users are kept up to date through a security education and awareness program. Last, but not least, know your assets, identify your perimeter of secure operations, and maintain a high level of situational awareness to ensure you are aware of, and can respond to, incidents in a timely manner for the sake of operational survival.

ENSURING RESILIENCY AGAINST CRITICAL INFRASTRUCTURE CYBER ATTACKS

Yes, Stuxnet is very sophisticated; and yes, it has the potential to cause damage. But it also has several weaknesses. First, it was found; second, it was highly specific; and third, that level of sophistication does not come cheap and may be difficult to replicate. But these weaknesses are not reasons for complacency. There is much we can learn from this attack and much we can do to lessen the impact of a similar attack. Symantec recommends the following steps be taken in order to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.
- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.
- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.

- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

EDUCATION IS A KEY COMPONENT TO SECURING CRITICAL SYSTEMS FROM CYBER ATTACK

But technology alone does not solve all the ICS vulnerability problems. After all, if that were the case, there would be far fewer breaches now with all the technological advances. People, processes, organization and technology must all be addressed. The question being asked of security professionals associated with U.S. critical national infrastructure is what should they be doing in response to the recent discovery of Stuxnet? We believe that the answer in part is related to education and awareness and Symantec sees this topic being broken down into a number of areas:

- Education in the classroom, where tomorrow's software developers and network architects can be found. We need them to think security from the outset.
- Education in colleges and the commercial education aftermarket, where people learn how to write software and learn how to design and manage networks. Security needs to be a byword.
- Education at the board level to convey the message that security should be primarily business-led and that support is required to ensure security is part of an organization's ethos - so security is led from the top. Understanding (from a business perspective) the threats and risks to an organization and how these interact with the cyber world is key to this understanding.
- Education at the management level to ensure the message that good security requires secure software and well-designed and maintained networks. In other words, security must be baked in from the outset and part of this is ensuring that staff skillsets are maintained appropriately and continuously. It is key to understand the risks and threats to an organization and be able to translate and/or augment the board's view of risk and threat into action plans.
- Finally, the security professional needs to be just that. Skillset maintenance is not an option, belonging to professional organizations is not an option, interfacing and carrying the security message to the board, management and staff level is not an option. That professional must be comfortable with assessing the risks to an organization based on what is on the ground and input from the board, management and industry. Being able to translate a risk assessment into a security get-well program and/or continuous security improvement programs is a key part of the security professional's job.

SYMANTEC 2010 CRITICAL INFRASTRUCTURE PROTECTION SURVEY

Our nation's critical information infrastructure is characterized as businesses and industries whose importance is such that if their cyber networks were successfully breached and disabled, it could result in a threat to national security. In the U.S., upwards of eighty-five percent of the nation's critical infrastructure is owned by the private sector. Symantec commissioned a recent study about critical infrastructure protection. The goal of Symantec's *2010 Critical Infrastructure Protection (CIP) Survey* was to find out how aware critical infrastructure companies were of government efforts in this area and how engaged and enthusiastic private enterprise was about working with government.

Symantec conducted the survey in August 2010 that included 1,580 enterprises in 15 countries worldwide, with companies ranging from 10 employees to more than 10,000. The median company had between 1,000 and 2,499 employees. We focused on six key critical infrastructure segments: Energy, Banking and Finance, Communications, Information Technology, Healthcare, and Emergency services. Symantec's *2010 Critical Infrastructure Protection (CIP) Survey* included the following highlights:

- **Critical infrastructure providers are being attacked.** Fifty-three percent of companies suspected experiencing an attack waged with a specific goal in mind. Of those hit, the typical company reported being attacked 10 times in the past five years. Forty-eight percent expect attacks in the next year and 80 percent believe the frequency of such attacks is increasing.
- **Attacks are effective and costly.** Respondents estimated that three in five attacks were somewhat to extremely effective. The average cost of these attacks was $850,000.
- **Industry is willing to partner with government on CIP).** Nearly all of the companies (90 percent) said they have engaged with their government's CIP program, with 56 percent being significantly or completely engaged. In addition, two-thirds have positive attitudes about programs and are somewhat to completely willing to cooperate with their government on CIP.
- **Room for readiness improvement.** Only one-third of critical infrastructure providers feel extremely prepared against all types of attacks and 31 percent felt less than somewhat prepared. Respondents cited security training, awareness and comprehension of threats by executive management, endpoint security measures, security response, and security audits as the safeguards that needed the most improvement. Finally, small companies reported being the most unprepared.

HOW GOVERNMENTS CAN ENHANCE CRITICAL INFRASTRUCTURE PROTECTION

Symantec would like to offer the following recommendations as the Committee considers how the U.S. government can further enhance its efforts to promote critical infrastructure protection including:

- Governments should continue to make resources available and partner with industry to establish critical infrastructure protection programs.
  - The majority of critical infrastructure providers confirm that they are aware of critical infrastructure programs.
  - Furthermore, a majority of critical infrastructure providers support efforts by the government to develop protection programs.
- Governments should partner with industries and industry organizations to develop and disseminate information to raise awareness of CIP organizations and plans. Specific information should include how a response would work in the face of a national cyber attack, what the roles of government and industry would be, who the specific contacts are for various industries at a regional and national level, and how government and private business would share information in the event of an emergency.
- Since most of the nation's cyber infrastructure is not government owned, a public-private partnership of government, corporate and private stakeholders is required to secure the Internet. Symantec commends the Department of Homeland Security for their engagement with the private sector. Under the National Infrastructure Protection Plan construct, DHS is the lead federal department for engaging

with the IT Sector. DHS has been a valuable partner to Symantec and the private sector, through the Sector Coordinating Councils (SCC) as well as the IT Information Sharing and Analysis Center (IT-ISAC)[6].

- Symantec has provided input to DHS on a number of "Comprehensive National Cyber Initiative" projects and we've also been engaged with the Department on several other cyber policy initiatives around the development of the National Cyber Incident Response Plan (NCIRP) including: resiliency, incentives, metrics, risk assessments, information sharing, and cyber exercises. In addition, we recently participated in the National Cyber Exercise, Cyber Storm III, which demonstrated the value of operational incident collaboration across the public and private sectors. Further, we've held several briefings with DHS to share expertise on Stuxnet and how critical infrastructures can better secure their systems against such threats. We look forward to continuing to partner with DHS and other agencies on the many issues and preparedness activities related to the nation's critical infrastructure protection.
- Governments should emphasize that security alone is not enough to stay resilient in the face of today's cyber attacks. In addition, critical infrastructure providers and enterprises in general should also ensure that their information is stored, backed up, organized, prioritized, and that proper identity and access control processes are in place.

CONCLUSION

Critical infrastructure industrial control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Stuxnet demonstrates that industrial control systems are more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Further, as demonstrated by past attacks and incidents involving industrial control systems, the impact on a critical infrastructure could be substantial.

Critical infrastructure control systems are more vulnerable today than in the past due to the increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems. Further, it is not uncommon for control systems to be configured with remote access through either a dial-up modem or over the Internet to allow remote maintenance or around-the-clock monitoring. If control systems are not properly secured, individuals and organizations may eavesdrop on or interfere with these operations from remote locations. Such pre-cautions would certainly prevent, limit or contain the threats posed by Stuxnet and similar malware.

Multiple private sector entities such as critical infrastructure industry organizations, trade associations, and standards setting organizations specific to the electric, chemical, oil and gas, and water sectors are working to enhance industrial control system security. These entities are developing standards, providing guidance to members, and hosting workshops on control systems security. Over the past few years, federal agencies—including the Department of Homeland Security (DHS), the Department of Energy, the National Institute of Standards and Technology (NIST), and others—have initiated efforts to improve the security of critical infrastructure industrial control systems.

[6] Symantec currently serves in the role of chairing the Information Technology Sector Coordinating Council and sits on the Board of the IT-Information Sharing and Analysis Center. As one of the critical sector organizations identified under the US National Infrastructure Protection Plan, the IT SCC is recognized by DHS as the representative IT industry body for coordinating strategic activities and communicating the sector's views on infrastructure protection, response and recovery issues. The IT-ISAC is a non-profit organization of leading IT companies focused on providing a mechanism for the trusted exchange of information on cyber incidents, vulnerabilities, attacks, solutions and countermeasures.

Stuxnet certainly has demonstrated the importance of public private information sharing partnerships across the critical infrastructure community. While DHS has made strides to partner with control systems vendors through its ICS-CERT, it should build on its October 2009 "Strategy for Securing Control Systems" and enhance its control systems partnership by including the IT and IT security community, who have traditionally worked with the DHS US-CERT. Cross collaboration within DHS is the key to improved situational awareness and operational response, and DHS should continue its efforts to integrate these functions. Until there is greater coordination between IT and IT security vendors and the industrial control systems owners and operators, there is an increased risk that multiple organizations will conduct duplicative work and miss opportunities to learn from and collectively respond to threats. Given the importance of these issues, we recommend that DHS (1) further enhance information sharing on control systems vulnerabilities with the IT and IT security communities; and (2) continue to work on integrating its information sharing capabilities to improve situational awareness and operational response partnerships with industry.

In closing, I'd like to take this opportunity to convey Symantec's strong support of S. 3480, the Protecting Cyberspace as a National Asset Act. We believe that this important legislation will enhance and modernize our nation's overall cybersecurity posture in order to safeguard our critical infrastructure from attack. The bill also importantly recognizes cybersecurity as a shared government and private sector responsibility which requires a coordinated strategy to detect, report, and mitigate cyber incidents. We look forward to continuing to work with the Committee to help advance this important legislation.

Symantec would like to thank the Committee for the opportunity to testify today. We remain committed to continuing to work in coordination with Congress, the Administration and our private sector partners to secure our nation's critical infrastructure from cyber attack. Thank you.

Written Statement
On behalf of
The Dow Corning Corporation and
The American Chemistry Council

Presented by

Mark W. Gandy, CISSP

Global Manager - IT Security and Information Asset Management

Dow Corning Corporation, Midland, MI 48686

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

Oversight Hearing on Nov. 17, 2010

"Securing Critical Infrastructure in the Age of Stuxnet."

Introduction

The American Chemistry Council (ACC) represents the leading chemical companies in the United States who produce the essential products critical to everyday life. The business of chemistry is a critical aspect of our nation's economy; employing nearly 803,000 Americans and producing more than 19 percent of the world's chemical products. In fact, more than 96% of all manufactured goods are directly touched by the business of chemistry. ACC members provide the chemistry used to produce lifesaving medications and medical devices; the body armor used by our men and women in the military and law enforcement; the light weight components for vehicles that help improve gas mileage; the energy saving building insulation and windows; silicon for solar panels and the durable, light weight wind turbine blades that help provide green energy.

Cyber Security is a Top Priority for ACC and the Chemical Sector

Because of our critical role in the economy and our responsibility to our communities, security continues to be a top priority for ACC members. Along with physical security, ACC members began actively addressing cyber security issues before and after the attacks of September 11, 2001.

In 2001, our members voluntarily adopted an aggressive security program that became the Responsible Care® Security Code (RCSC). Responsible Care implementation is mandatory for all members of the ACC. The RCSC is a comprehensive security management program that addresses both physical and cyber security and requires a comprehensive assessment of security vulnerabilities and risks and to implement protective measures across a company's value chain. A company's security plan is reviewed by an independent, credentialed third-party auditor. The RCSC has been a model for state-level chemical security regulatory programs in New Jersey, New York and Maryland and was deemed equivalent to the U. S. Coast Guard's Maritime Transportation Security Act (MTSA).

Since RCSC's inception, ACC members have invested more than $8 billion in security enhancements including both physical and cyber security protections. Security in all its dimensions continues to be a top priority for ACC and the chemical industry, and our record of accomplishment and cooperation with Congress, DHS and others is undisputed.

In June 2002 ACC members began implementation of the Chemical Sector Cyber Security Strategy, which was referenced by the Bush Administration's National Strategy to Secure Cyberspace of 2003. ACC was gratified that in 2009 the Obama Administration made cyber security a top priority. ACC participated in the White House 60-Day Cyber Policy Review and our cyber experts work closely with the DHS National Cyber Security Division (NCSD) in many areas including: national Cyber Storm exercises, information sharing programs, development of the "Roadmap to Secure Control Systems in the Chemical Sector." A 2009 Program Update can be found on the Obama Administration's website - "Making Strides to Improve Cyber Security in the Chemical Sector."

Public/Private Partnerships are Essential to Securing Cyber Systems in the Chemical Sector

The Chemical Sector continues to work with and align its priorities with those of the Department of Homeland Security (DHS) in order to advance the cyber security agendas of both organizations. The National Cyber Security Division (NCSD) of DHS is the government agency with primary responsibility for working with public, private and international entities to secure cyberspace and America's critical cyber assets. Over the last several years, the chemical sector has closely aligned its efforts with NCSD initiatives and plans to continue to provide sector representation in the following NCSD venues and others that may be created in the future. Examples of this alignment include:

- Cross-Sector Cyber Security Working Group (CSCSWG)

- Industrial Control Systems Joint Working Group (ICSJWG)
- National Security Exercises

In addition, the chemical sector works closely with other DHS divisions that focus on facility and transportation security issues to ensure that cyber security components of their work are appropriately addressed. These divisions include:

- Infrastructure Security Compliance Division (ISCD)
- Chemical Sector-Specific Agency (SSA)
- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

Chemical Facilities Anti-terrorism Standards (CFATS)

On April 9, 2007 the U. S. Department of Homeland Security promulgated the "Chemical Facilities Anti-Terrorism Standards" (CFATS) regulatory program. This comprehensive Federal program requires high-risk chemical facilities to register with DHS, conduct a thorough site security assessment and implement protective measures that comply with 18 risk based performance standards (RBPS). In particular, RBPS #8 addresses performance for cyber security, requiring high-risk facilities to develop the capability to effectively deter and prevent cyber sabotage, including unauthorized on-site or remote access to critical process controls. RBPS #8 identifies the following policies and practices to effectively secure cyber systems from attack or manipulation: security policy, access control, personnel security, awareness and training, monitoring and incident response, disaster recovery and business continuity, system development and acquisition, configuration management, and audits.

Additionally, CFATS requires enhanced security measures for critical cyber systems that monitor and/or control physical processes that contain a chemical of interest (COI) or that include critical business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI.

In early 2010, DHS began inspecting covered high risk chemical facilities starting with Tier 1 sites that pose the highest risk.

Development of International Standards

Sustained and long-term improvements in the security of industrial control systems will only be achieved through the definition and application of well-defined and accepted international standards. Our sector is leading in the development of comprehensive international standards by the International Society for Automation (ISA), an organization that brings together owner-operators, technology providers, researchers and a several other constituencies.

Several of these standards have been published and accepted by the International Electrotechnical Commission (IEC), and several more are under active development. These standards are by design applicable to all sectors that employ industrial control systems.

The Roadmap to Secure Control Systems in the Chemical Sector

Published in September 2009, the "Roadmap" was developed in partnership with the Department of Homeland Security and the chemical sector. It provides a template for action as industry and government work together to achieve a common goal of securing industrial control systems in the chemical sector by establishing specific goals and objectives and milestones over a 10 year journey. In the desired state, all U.S. chemical sector companies will be actively working to achieve common cyber security goals. Additionally, using the latest practices and guidance will be an inherent part of company cyber security programs to help ensure proper controls are in place to protect company systems and information. Finally, the sector will have solid working relationships with strategic technology providers and government agencies. Key elements of the Roadmap include:

1. **Information sharing**

Information sharing will be seamless within the chemical industry, between the chemical sector and government agencies including the Department of Homeland Security (DHS) and among critical infrastructure sectors at a strategic, tactical and operational level. United States cyber security activities will be coordinated with global efforts to enhance chemical sector performance worldwide. Chemical companies will be comfortable sharing appropriate yet security-sensitive information with DHS and industry counterparts.

2. **Guidance enhancement and relevance**

Chemical companies have access to new and improved practices, resources and standards created by external organizations and/or the Chemical Sector Cyber Security Program to help them address maturing cyber security needs and legislative requirements. Chemical Sector Cyber Security guidance documents will remain evergreen through periodic reviews and will be available to assist chemical companies in enhancing their cyber security preparedness and performance as well as compliance with the CFATS regulations.

3. **Sector-wide adoption**

Cyber security is recognized as a critical aspect of overall security and is addressed in coordination with physical and transportation security within the chemical industry. The increased emphasis on cyber security will lead all chemical trade associations to incorporate cyber security practices as a condition of membership within existing product stewardship programs or security programs. Additionally, the sector's activity will be managed through one consistent, coordinated program.

4. **Enhanced security in technology solutions**

Suppliers of IT products and services are best positioned to address issues within the solutions they create and have a responsibility to test and enhance product security before releasing items into the marketplace. Information technology suppliers will design their solutions to maintain highly-available systems, support future versions of these long-lived assets and meet governmental compliance standards. They will also make a more formal commitment to product reliability, integrity and security, thus more fully embracing the philosophy of secure by design.

Cyber Storm III and National Exercises

In September of 2010, DHS held its third National Exercise focused specifically on Cyber Security. Since its inception ACC and the Chemical Sector was actively involved in its planning, preparation and execution. Cyber Storm III participants included Federal, State and local governments; private sector companies; and International partners. In addition to the chemical sector, significant emphasis was also placed on the IT, Tele-communication, Electric and Transportation sectors.

The Chemical Sector objectives through Cyberstorm III were focused on testing its ability to effectively activate the ACC Cyber Incident Response Plan (CIRP). The CIRP was developed to effectively mobilize the chemical sector in responding to a significant cyber security event having national and regional impacts to economy and to public safety.

Overall Cyber Storm III Exercise Objectives were:

1. Exercise the National Cyber Incident Response Plan (NCIRP)
2. Examine the role of the DHS in a global cyber event
3. Focus on information sharing issues (requirements, classified/tear-line, etc, information condition/alert levels, thresholds, response roles & responsibilities, authorities)

4. Examine coordination and decision-making procedures/mechanisms across the constituency (Federal, state, private sector, international)
5. Practically apply findings from past exercises

National level exercises are crucial to testing the capability of the chemical sector to respond effectively in the event of a national emergency and to identify gaps and areas for improvement. ACC will be working to address the learnings from Cyber Storm III to ensure that our industry continues to take the appropriate steps to enhance our preparedness of cyber incidents.

Conclusion

The above activities and programs demonstrate the chemical sector commitment to the advancement of cyber security in the critical infrastructure. This commitment has been consistent and sustained for almost a decade and has led to the creation of very effective working partnerships within our sector, across sectors, and with the government.

Post-Hearing Questions for the Record
Submitted to Seán P. McGurk
From Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"
November 17, 2010

Question#:	1
Topic:	Stuxnet
Hearing:	Securing Critical Infrastructure in the Age of Stuxnet
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: The earliest sample of Stuxnet was discovered on Siemens Programmable Logic Controllers (PLCs) in June 2010. Today, experts are still analyzing the code to understand Stuxnet's features and its intent and to identify systems that have been infected.

Based on the cyber threat landscape and the insight that you bring from government, industry, and research, how would you characterize the level of preparedness and awareness in the private sector to deal with threats like Stuxnet?

Response: The Department of Homeland Security (DHS) learned about the Stuxnet threat in June of 2010 and has been working closely with the private sector. Together tremendous progress has been made. However, preparation for threats such as Stuxnet remains difficult. Stuxnet's highly sophisticated and advanced nature, which includes the use of zero-day exploits, digitally signed certificates, and other anti-evasion and detection techniques, makes Stuxnet a "game changer." Given that zero-day exploits are unknown vulnerabilities for which no security fix is available, threats such as Stuxnet pose an immense challenge. The private sector's current preparedness and awareness levels vary considerably both across and within the 18 Critical Infrastructures/Key Resources (CIKR), thus increasing the difficulty of responding to an advanced threat such as Stuxnet.

Some private sector organizations have placed a significant focus on preparedness and awareness of cybersecurity threats, yet the level of preparedness of individual organizations within each sector varies widely. Some organizations have demonstrated sophisticated knowledge of cyber threats, and have developed procedures and technologies to help them prevent and respond to such threats, including dedicated staff assigned to detect and respond to incidents. Others lack the requisite understanding, necessary resources, and appropriate skill sets to meet challenges posed by the current

Question#:	1
Topic:	Stuxnet
Hearing:	Securing Critical Infrastructure in the Age of Stuxnet
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

and future threat landscape, and are struggling with implementing effective incident response processes and plans.

What Stuxnet succeeded in doing was raising awareness of the criticality of control systems, highlighting the interdependencies and vulnerabilities that exist in these legacy environments and demonstrating there are motivated groups of individuals who are interested in carrying out cyber attacks on these systems. Consequently, awareness of cyber threats is at an all-time high and many CIKR owners and operators within the private sector are placing a heavy focus on better preparing themselves for the "next Stuxnet" threat. The recognition of diverse control systems vulnerabilities to Stuxnet and similar cybersecurity threats has manifested into a growing interest by the private sector and the Department of Homeland Security's (DHS) Control Systems Security Program and its various products and services, such as onsite assessments, control system security training offerings, and the Industrial Control Systems Computer Emergency Response Team (ICS-CERT). Through in-house expertise and close working relationships with Government and private industry partners, the Department's capabilities will continue to advance the state of both preparedness and awareness to help protect critical industrial control systems from current and future cybersecurity threats.

Question#:	2
Topic:	sharing
Hearing:	Securing Critical Infrastructure in the Age of Stuxnet
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Information sharing is key to preventing, detecting, and responding to cyber incidents. Identifying the threat and an effective response is only possible with timely information sharing between all stakeholders.

From your perspective, how would you characterize the effectiveness of information sharing with regard to Stuxnet within the private sector and between the private sector and the government?

Response: Stuxnet was a prime example where effective coordination was an integral part of the response effort. The Department of Homeland Security (DHS) utilizes information sharing portals to share secure information, disseminate threat and vulnerability warnings and alerts and collaborate with Government and private sector partners through Information Sharing and Analysis Centers (ISACs), Secret Service Electronic Crime Task Forces (ECTFs) and focused working groups to provide essential and timely information to all customers and partners. DHS also worked directly with the vendor community, including Microsoft and Siemens, to validate their mitigation strategies and assist with communicating these actions/requirements to the broader stakeholder community. While DHS works diligently to provide information to the private sector, we continue to look for ways to enhance our information sharing practices.

Serious threats such as Stuxnet continue to require effective and timely coordination and information sharing across all sectors. DHS is addressing this challenge through the National Infrastructure Protection Plan (NIPP) and building capable programs dedicated to reducing overall risk to the nation's critical infrastructure through raising awareness and offering support when requested/needed. Today, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Control Systems Security Program continue to dedicate resources and capabilities to increase awareness, share information with various partners, and bridge communications between public and private sectors to adapt and effectively respond to evolving cybersecurity threats across the Nation.

Responses to Post-Hearing Questions for the Record
Submitted to Michael J. Assante
From Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"
November 17, 2010

Submitted by Michael J. Assante on January 2, 2011

1. The earliest sample of Stuxnet was discovered on Siemens Programmable Logic Controllers (PLCs) in June 2010. Today, experts are still analyzing the code to understand Stuxnet's features and its intent and to identify systems that have been infected.

   Based on the cyber threat landscape and the insight that you bring from government, industry, and research, how would you characterize the level of preparedness and awareness in the private sector to deal with threats like Stuxnet?

   Response by Michael J. Assante:

   I believe the general level of awareness about potential vulnerabilities from cyber threats like Stuxnet has been growing in both government and industry, but the awareness lacks an understanding of how systems are being compromised and what is ultimately possible or even probable. I saw a good degree of change while I was at NERC as the industry worked to understand the issue and its impact on system reliability. A very important initiative that begins to define the problem is the recent joint report by NERC and the U.S. Department of Energy ("DOE"), entitled *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* This start must be followed by focused outreach and honest information sharing to uniformly develop an understanding of the problem and its implication on safe and reliable power generation and delivery.

   My response to the question of awareness indicates the level of preparedness to be less mature than it needs to be. One can't be optimally prepared for a problem that is not fully understood, as many of the incredible response capabilities of individual utilities are not best aligned to the challenges of responding to a sophisticated cyber event. It is important to note that no large-scale power outage has ever been attributed to a physical or cyber attack in North America. This can't be said for the necessary operations of electricity control and system monitoring technology, which have been noted as contributors to outages. Our limited history and the deceptive reliance on digital technology have led to a state of inadequate preparedness to the new vulnerabilities introduced by this growing reliance. The Stuxnet worm is a capability that was not considered possible in the design of cybersecurity reliability standards or industry security guidelines and practices. There is much work to be done.

2. Information sharing is key to preventing, detecting, and responding to cyber incidents. Identifying the threat and an effective response is only possible with timely information sharing between all stakeholders.

   From your perspective, how would you characterize the effectiveness of information sharing with regard to Stuxnet within the private sector and between the private sector and the government?

   Response by Michael J. Assante:

   The private sector's access and willingness to share information is not as effective as it should be to allow for the development of timely, efficient, and effective cyber security measures. The discover of the Stuxnet Worm and subsequent timeline of information disclosure and dissemination regarding the capabilities and potential targets of the worm demonstrate the importance of developing more effective information sharing. It took months to develop and share an accurate understanding of the Stuxnet Worm with very little actionable information available during the first few weeks that could support effective risk mitigation decision-making. For the purposes of developing lessons learned, an investigation should be undertaken to understand what information was made available by relied upon risk communicators and authoritative parties and how that information was shared among government agencies and the potentially vulnerable parties in the private sector. I was disappointed by the information that was made available by organizations relied upon by the industry, such as the effected control system vendor and by computer security response organizations that focused on the non-control system portion of the Stuxnet code. In contrast to this individuals and unexpected organizations began to fill the gap as highlighted by the incredible work accomplished by Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien and control system experts, like Ralph Langner. They began to analyze the code with little assistance from organizations established to work these types of problems and were willing to share and publish their findings. Their publishing of information and findings provided more effective information sharing and provided details that were not found in traditionally relied upon sources of this type of information.

   A mixed track record of providing value and a certain level of distrust surrounding the ultimate use and safeguarding of the information hinder private sector and government sharing capabilities. I believe the government might be able to build an effective collaborative relationship with industry if they can start delivering information that is timely and of value. This relationship must emphasize that non-government channels can often be more effective as they are less constrained and may have greater acceptance by industry. The dilemma is developing a process that can be qualified over time to identify sources that are credible. An effected entity is in a difficult position waiting for deliberate and authoritative sources or trying to vet more timely information sources provided by a global community of experts. We now live in a specialized world where different elements of necessary risk mitigation information reside in a far greater number of diverse, and sometimes geographically distant, places around the globe. Our ability to effectively assemble both expertise and proper context, along with an acceptable degree of verification, will significantly improve our ability to protect systems and minimize the effects of cyber weapons.

I testified to the problem of too much information being restricted to national security community members without clear guidance that allows for necessary and actionable information to be made available to both affected entities and security agencies while protecting sources and capabilities. I believe organizations responsible for working with the private sector to reduce cyber risk should be measured on their ability to communicate valuable and actionable information in a timely manner. The Department of Homeland Security and the intelligence community must develop more effective processes that focus on delivering relevant and actionable information to the private sector. Industry and technology experts able to address context, priorities/importance, and pitfalls must be engaged to inform these processes. The Department of Defense and intelligence community went through a self-directed transformation to prioritize intelligence being collected, analyzed, and reported to support the war fighter. Organizations like the Industrial Control Systems CERT need to prioritize information collection, analysis, and reporting to better support the critical infrastructure defender community. The demands from other federal organizations and funding sources can easily supersede the less definable and expansive community of infrastructure owners and operators, measuring their success should include direct feedback from the targeted customer.

Finally, information sharing should occur after an event or incident not just during an event. There is a lot of value to bringing both parties together in a more organized fashion after a crisis to learn from each other. This will provide a more complete perspective and understanding to drive research and development, identify areas of concern, highlight opportunities, and lay the foundation for future information sharing and innovation.

Post-Hearing Questions for the Record
Submitted to Dean Turner
From Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"
November 17, 2010

1. According to a Symantec white paper on Stuxnet, the overwhelming majority of total infected systems were found in Iran and only a small percentage in the United States. Some attribute this to the intent of the attack, saying that it was programmed to target Iran and its designers wanted to keep its scope contained.

   If an advanced threat like Stuxnet had actually targeted critical infrastructure in the United States, it could do serious harm. However, we can minimize damage and preserve the operation of critical infrastructure by developing emergency plans in advance and having robust information-sharing mechanisms in place.

   Could you describe how DHS engaged with Symantec or the chemical industry after Stuxnet was discovered in late June?

2. Information sharing is key to preventing, detecting, and responding to cyber incidents. Identifying the threat and an effective response is only possible with timely information sharing between all stakeholders.

   From your perspective, how would you characterize the effectiveness of information sharing with regard to Stuxnet within the private sector and between the private sector and the government?

The responses to these Questions for the Record were not received at time of printing.

Post-Hearing Questions for the Record
Submitted to Mark W. Gandy
From Senator Susan M. Collins

"Securing Critical Infrastructure in the Age of Stuxnet"
November 17, 2010

1. According to a Symantec white paper on Stuxnet, the overwhelming majority of total infected systems were found in Iran and only a small percentage in the United States. Some attribute this to the intent of the attack, saying that it was programmed to target Iran and its designers wanted to keep its scope contained.

If an advanced threat like Stuxnet had actually targeted critical infrastructure in the United States, it could do serious harm. However, we can minimize damage and preserve the operation of critical infrastructure by developing emergency plans in advance and having robust information-sharing mechanisms in place.

Could you describe how DHS engaged with Symantec or the chemical industry after Stuxnet was discovered in late June?

While we are not familiar with the specific engagement between DHS and Symantec, we are familiar with the outreach that DHS continues to provide to the chemical sector on Stuxnet. Much of the information about the nature of the Stuxnet attack was first available from various private sector researchers and industry experts. However, DHS did provide summaries and overviews of the information that probably reached many people who may not have previously seen the information.

DHS through its National Cyber Security Division and US Cert has engaged the private sector on information related to the Stuxnet attack through participation at industry conferences, meetings and workshops. For example, DHS participated in the American Chemistry Council's ChemITC Conference this fall and provided an informative briefing on the latest knowledge related to the Stuxnet attack at an unclassified level.

While DHS continues to provide useful information on such events, timely information sharing on current cyber threats could be enhanced through the creation of cyber-security information networks both at classified and unclassified levels. More work can be done to ensure that more cyber security experts in the private sector have security clearances. This is particularly true in the Chemical Sector. And lastly, ACC believes that the Government can do a better job of sharing information with itself across the various agencies that collect and analyze intelligence. Again, while this has improved vastly since September 11, 2001, more work needs to be done. ACC stands ready to assist the DHS and Congress to help further improve information sharing at all levels.

2. Information sharing is key to preventing, detecting, and responding to cyber incidents. Identifying the threat and an effective response is only possible with timely information sharing between all stakeholders.

   From your perspective, how would you characterize the effectiveness of information sharing with regard to Stuxnet within the private sector and between the private sector and the government?

   Information sharing within the private sector, between those who are heavily involved in control systems security, has been excellent. This has included researchers, vendors, consultants and owner-operators. The community of experts on industrial control systems security is quite small and as a result the trust level is quite high. This contributes to the increased sharing of information, albeit in an informal fashion.

   Much of the information on Stuxnet was also available to DHS as it became public. However, perhaps because of concerns about its sensitive nature, less detail information on Stuxnet has come from the Government. It appears there has been considerable sharing of information between DHS and the vendor community.

3. The Cyber Storm III exercise conducted by DHS in September tested the newly-developed National Cyber Security Incident Response Plan (NCIRP) to examine the roles, responsibilities, authorities, and management capabilities of the plan.

   You participated in Cyber Storm III as a representative of the chemical sector. What were the primary lessons learned from this experience for the chemical sector?

   One of the main goals of Cyber Storm III was to test the ability of the private sector to effectively share information during a crisis. ACC used this opportunity to test our own Cyber Incident Response Plan and Communication Tool. ACC was encouraged by the performance of its CIRP, which enabled ACC members to quickly assemble and share information on a regular cycle while the emergency was ongoing. It was also quite effective in identifying and engaging the public sector including the DHS Chemical Sector SSA, the NCSD, US Cert and the newly created Unified Coordination Group.

   Some areas for improvement in ACC's CIRP tool were identified as well, including a need to streamline communications within the private sector. ACC believes that enhanced communication with the broader membership of the Chemical Sector Coordinating Council (CSCC) could be useful. As a first step, ACC helped to establish the Cyber Security Implementation Workgroup of the CSCC. The Workgroup's initial focus is implementation of the Chemical Sector Cyber Security Roadmap. By engaging the sector as a whole, ACC believes information sharing can be vastly improved thus accelerating the state of secure cyber systems in the chemical sector.