[H.A.S.C. No. 112–5]

WHAT SHOULD THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER BE?

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS
AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

HEARING HELD
FEBRUARY 11, 2011

U.S. GOVERNMENT PRINTING OFFICE
64–861 WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
CHRIS GIBSON, New York
BOBBY SCHILLING, Illinois
ALLEN B. WEST, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California

JAMES R. LANGEVIN, Rhode Island
LORETTA SANCHEZ, California
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
TIM RYAN, Ohio
C.A. DUTCH RUPPERSBERGER, Maryland
HANK JOHNSON, Georgia
KATHY CASTOR, Florida

Kevin Gates, *Professional Staff Member*
Mark Lewis, *Professional Staff Member*
Jeff Cullen, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2011

FRIDAY, FEBRUARY 11, 2011

WHAT SHOULD THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER BE?

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

WHAT SHOULD THE DEPARTMENT OF DEFENSE'S ROLE IN CYBER BE?

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Friday, February 11, 2011.

The subcommittee met, pursuant to call, at 11:30 a.m., in room 2118, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. Hearing will come to order.

Let me welcome the members and witnesses and guests to this first hearing in this Congress of the Emerging Threats and Capabilities Subcommittee.

I certainly appreciate all the members who have chosen to join this subcommittee. And among other benefits, we will have the former chair and former ranking member of the subcommittee, Ms. Sanchez and Mr. Miller, as part of our body.

But I am really looking forward to the chance to working in partnership with the gentleman from Rhode Island, Mr. Langevin. He and I started working together on cyber issues in 2003 as part of the Select Homeland Security Committee, on the Cyber Subcommittee of that body, and have worked together on this committee and on the Intelligence Committee basically ever since. So I look forward to what we can accomplish together for the country's security in the next two years.

One of the first things that one notices is the name of the subcommittee has changed. And I think that is to better match what our charge is. We are to look out in the future and help see that the United States is prepared to deal with those national security challenges that are still emerging, that we are still learning about. Things such as terrorism and cyber warfare.

We are also charged with nurturing emerging capability that can meet those and other threats. And the jurisdiction of the subcommittees has been changed to reflect so we can better focus on cyber and these other challenges.

Of course, any emerging threat presents new challenges on policy, legal authority, budgeting, such as we have witnessed, for example, since 9/11. And today, in the field of cyber, we want to start by asking really a fairly basic but I think important question, and that is, what is the role of the Department of Defense in defending the country in cyberspace?

If a formation of planes or some hostile-acting ships came barreling towards a factory or refinery in the U.S., I think most of us have a pretty good idea of what we would expect from the Department of Defense. They may try to identify who it is, divert them over to another area. They may even go so far as to shoot them down. But the bottom line is we expect our military to protect us from threats that we cannot handle on our own.

But what do we expect, or what should we expect, if a bunch of malicious packets, or potentially malicious packets, come barreling at us—or come barreling at the same facilities in cyberspace? I am not sure we have a good answer to that. And if we figure out what we expect, then the question is, can the government do what we expect? Does it have the ability and the authorization to do it?

I don't expect that we are going to get definitive answers to those questions today, but I do think we need to be serious and diligent about pursuing those answers because the threat is serious and it is growing in numbers and sophistication.

Yesterday, at the Intelligence Committee hearing, I asked DNI [Director of National Intelligence] Clapper, Director Panetta, FBI [Federal Bureau of Investigation] Director Mueller about how serious the threats in cyberspace were as a matter of national security. Each of them responded they thought it was in fact very serious. Clapper said, "The threat is increasing in scope and scale, and its impact is difficult to overstate."

So we know that cyber is a new domain of vandalism, of crime, of espionage, and, yes, even warfare, but I am afraid the country is not very well equipped to deal with any of those challenges.

As we look for solutions, we have to be smart and careful and true to our values, but I believe we need to act to improve our security.

And I appreciate the witnesses who are here today to help guide us on that path.

But first, I would yield to the distinguished gentleman from Rhode Island, the ranking member, for any comments he would like to make.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 33.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Well, thank you, Mr. Chairman.

As this is our subcommittee's first hearing of the 112th Congress, I just wanted to take a moment to congratulate you on your chairmanship and to say how much I very much looking forward to working with you again. As you rightly pointed out, we have worked on many of these issues together in our time on the Homeland Security Committee, to our time as we have served on this committee, and as well as the House Intelligence Committee.

So our paths keep crossing in a very positive way and we have enjoyed a very productive partnership in the past and I know we will continue with our work on this subcommittee as well. So congratulations to you.

In 2007, as chair of the Homeland Security Subcommittee on Emerging Threats, Cyber Security and Science and Technology, I conducted a detailed and thorough examination of cyber threats to our power grid after tests conducted at Idaho National Labs, known as Aurora, became public.

At that time, industry representatives from NERC [the North American Electric Reliability Corporation] misled or were inaccurate about their testimony to the Homeland Security Committee about their efforts to address these threats in the private sector. Now, we called them on it and they retracted their statements. But the experience illustrates how difficult it can be to require and ensure security when it comes to critical infrastructure.

Since then, threats to our critical infrastructure have only grown, with news reports suggesting that there is interest by malicious actors in exploiting vulnerabilities in the U.S. power grid and other critical infrastructure. The federal agencies have taken steps to reduce these vulnerabilities. I have to say, though, I am afraid that many in industry and in government still fail to appreciate the urgency of this threat. Since I began working on this issue, I have been disappointed by the overall lack of serious response and commitment to this issue, and I still believe America is vulnerable to a cyber attack against the electric grid that would cause severe damage not only to our critical infrastructure, but also to our economy and the welfare of our citizens.

Because of this concern, last Congress I posed this question to the heads of all of our military services. If our civilian power system is vulnerable, what is being done to protect our numerous military bases that rely on them to operate?

Well, the answers were disturbing, but not surprising. Vice Admiral Barry McCullough, head of the Navy's 10th Fleet, testified that, "These systems are very vulnerable to attack," noting that much of the power and water systems for our military bases are served by single sources and have only very limited backup capabilities with an attack on a power station potentially requiring weeks or even months to recovery from, our bases could face serious problems maintaining operational status. A recent report from the Department of Energy's Inspector General found that despite years of concern and hand-wringing by those who are aware of the threat, not much has been done to increase protection to these civilian systems.

Their reports also fault federal regulators for not implementing the adequate security standards—cyber security standards. But if you ask industry, you will find out that there is no actual requirement to do what the government wants. The regulators don't have any actual ability to regulate when they see a problem, despite being fully aware of the tremendous risks that face our nation.

Now, if everyone is aware of the threat, both DOD [the Department of Defense] and our civilian power sector, it appears that the tragedy of the commons has ruled that no one has been willing or able to address it.

At the House Intelligence Committee's annual open meeting yesterday, Director Panetta testified that cyber threats to our critical infrastructure had the potential to be the next Pearl Harbor, and

I agree and remain unconvinced that we have the abilities or the authorities to stop a large-scale cyber attack.

To this end, last year I introduced legislation to coordinate our national cyber security policies for the protection of our federal networks, as well as our critical infrastructure. And while we had success with an amendment in the House defense authorization measure, you may know that we were forced to remove that language during conference.

Let me just say, Mr. Chairman, that I look forward to working with you to move forward again this year and finally begin to address these critical vulnerabilities.

Today, I am anxious to hear from our panel, especially Mr. Cauley from NERC and ask what has changed since 2007. Are we still as vulnerable today as we were then? And I, for one, believe that the answer is yes. I fear that little has changed other than the acceleration of the threat and the growth of our vulnerability.

With that, Mr. Chairman, I look forward to our witnesses' testimony. I want to thank our witnesses for being here, and I yield back.

Mr. THORNBERRY. I thank the gentleman.

And now we will turn to our witnesses. And let me say first of all, I appreciate each of you all's written statement. Without objection, they will be made part of the full record. But I thought each of you did a very good job in laying out a number of issues. I know I learned from each of them, so I appreciate the effort you put into that.

With us today is Dr. Shari Pfleeger, director of research from the Institute of Information Infrastructure Protection headquartered at Dartmouth; Mr. Gerry Cauley, chief executive officer of the North American Electric Reliability Corporation, NERC; and Mr. Gregory Nojeim, senior counsel, Center for Democracy and Technology.

Pretty good? Okay, good.

Thank you all for being here. We will try to move out smartly today. I don't think we will have votes for a little bit, and I would like to give everybody a chance to ask questions before those votes. So as I say, your full statement will be made part of the record, if you would like to summarize it, and then we will turn to questions.

Dr. Pfleeger, the floor is yours.

STATEMENT OF SHARI L. PFLEEGER, DIRECTOR OF RESEARCH, INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION AT DARTMOUTH COLLEGE

Ms. PFLEEGER. Good morning, Chairman Thornberry, Ranking Member Langevin, members of the subcommittee and guests. Thank you for inviting me here. I was asked to talk about the economics of cyber security and I have organized my response based on the three big questions that you asked me.

So the first one is: What are the significant challenges that face us? And I see three big challenges. The first is the diverse and distributed ownership of the cyber infrastructure, which makes it difficult to apply traditional approaches for security because there are so many different pieces. And many of those pieces have been developed without security in mind. They are not always the big—security is not always the biggest motivator for making money for the providers of those pieces.

The second is appeal as a criminal tool. Criminals can use the cyber infrastructure to perpetrate their crimes more broadly, more quickly and more anonymously than they could before.

And the third is, and this perhaps has the most relevance to the Defense Department, the difficulty in reaction to emergent behavior. Many aberrant cyber-based behaviors are emergent in that it takes a long time to figure out exactly what is going on, understanding the cause and effect, and selecting an appropriate reaction. And when the cause is uncertain and the possible responses have life-threatening or diplomatic implications, the decision-makers have to reduce the uncertainty surrounding cause and effect.

So I have identified three policy, legal, economic and technical challenges. The first is misaligned incentives. Most of the providers are in business to make money, not necessarily to provide security. And so many organizations prefer just to wait for cyber attacks to happen and clean up the mess, or they rely on what is sometimes called "free-riding" or "herd immunity," where they let other people implement the security, and the people who don't implement the security still get some benefit.

And in addition to that, the bad outcomes don't always affect the organization lacking security or don't affect them for very long. So, for instance, their stock prices might go down, but then they eventually pop back up again. So there is little incentive for them to take a long-term security view.

The second is the need for diversity. Technological diversity leads to more secure networks and systems, but because of a variety of things, including economic reasons, training, access and even chance, the technology is actually quite uniform, more than we would expect.

And finally, security is often incompatible with organizational culture and goals, so many people who use our networks are paid to get their jobs done and they often see security not as an enabler, but as an inhibitor. So you see lots of cases of people turning off the security in order to get their jobs done, or neglecting to do things like set the security properly.

So what should the government do? I suggest five things. The first is to address cyber attacks the way other unwelcome behaviors are addressed. Our current reliance on convenience surveys for information about cyber attack trends can be misleading and we need more careful sampling and more consistent solicitation of data.

The government should incentivize or require better breach, fraud and abuse reporting, and data about the nature and number of cyber attacks should be reported consistently each year so that sensible trend data can form the basis for effective actions. It may be more useful to capture data in smaller ways, in various ways for various purposes, and then good economic models informed by these representative consistent data can improve our general understanding not only of the cyber risk, but of the cyber risk relative to other kinds of risk.

Second, I recommend that liability statutes cover cyber technology. When lack of car safety was made more visible in the

1960s, the government responded by making automobile companies more liable for their unsafe practices and products. Similarly, I think a combination of manufacturer liability and economic constructs like insurance could encourage more secure product design and implementation.

The third is insist on good systems engineering. Use the government's purchasing power in two important ways. First, refuse to continue to deal with system providers whose products and services are demonstrably insecure, unsafe, or undependable. The data gathered in this process can inform subsequent technology decisions so that errors made in earlier products are less likely to occur in later ones. Especially in cyber security we see the same problems appearing over and over again.

Secondly, insist on five up-to-date formal arguments describing why the systems are secure and dependable. These arguments are used in other domains like nuclear power plant safety and could easily be applied to cyber security. And suppliers' formal arguments could be woven into the system integrator security arguments to show that supply chain issues have been addressed with appropriate levels of care and confidence.

The fourth suggestion is to provide incentives to encourage good security hygiene. Incentives like tax incentives and insurance discounts can speed implementation of demonstrably more security technology and the incentives should also include rewards for speedy correction of security problems and punishments for lax attention to such problems.

Finally, encourage multidisciplinary research. Many security failures occur not because there is no solution but because the solution hasn't been applied or because designers fail to include the user's perspective when designing the technology.

Research involving behavioral science and behavioral economics can improve the security and dependability of the nation's cyber infrastructure in two ways. In the short term, it can improve adoption rates for the security technology, thereby reducing the attack surface against which malicious actors aim. And in the longer term it can lead to a more resilient cyber infrastructure that users are eager to use correctly and safely.

Thank you.

[The prepared statement of Ms. Pfleeger can be found in the Appendix on page 34.]

Mr. THORNBERRY. Thank you.

Mr. Cauley.

STATEMENT OF GERRY CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. CAULEY. Good morning, Chairman Thornberry, Ranking Member Langevin, members of the subcommittee and fellow panelists. My name is Gerry Cauley. And referring to Ranking Member Langevin's comments on the performance of NERC in the past, I would point out that I am the new President and CEO of the North American Electric Reliability Corporation. And I also serve as the Chairman of the Electricity Subsector Coordinating Council.

I am a graduate of the U.S. Military Academy at West Point, a former officer in the U.S. Army Corps of Engineers. I have a master's degree in nuclear engineering from the University of Maryland. And I have devoted over 30 years to working toward the safety and reliability of our nuclear and electric industries, including in 2003 serving as a lead investigator for the 2003 Northeast blackout.

I have with me also today NERC's chief security officer, Mark Weatherford, behind me, who until recently served as the chief information security officer for the state of California and previously served 26 years in the U.S. Navy as an information security officer.

NERC is a non-profit corporation that was founded in 1968 to develop voluntary operating and planning standards for the owners and operators of the North American bulk power system.

In 2007, the Federal Energy Regulatory Commission designated NERC as the electric reliability organization in the United States, in accordance with the Energy Policy Act of 2005.

As a result, our standards, including cyber security standards, became enforceable at that time. To my knowledge, they are the only mandatory cyber standards among the various critical infrastructures in North America.

As CEO of the organization charged with overseeing reliability and security of the North American grid, I am deeply concerned about the changing risk landscape from conventional risks such as extreme weather and equipment failures to emerging new risks where we are left to imagine scenarios that might occur and prepare to avoid or mitigate the consequences, some of which could be more severe than we have previously experienced.

I am most concerned about physical and cyber attacks intended to disable elements of the power grid or deny specific electricity to specific targets such as government and business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries and are simply not random failures or acts of nature.

It is difficult to address such rapidly evolving risks solely with a traditional regulatory model that relies mainly on mandatory standards, regulations and directives.

The defensive barriers mandated by our standards do make it more difficult for those seeking to do harm to the grid, but alone they may not be completely sufficient in stopping the determined efforts of the adaptable adversaries supported by nation-states or organized terrorist groups.

The most effective approach against such adversaries is to apply resiliency principles as outlined in the National Infrastructure Advisory Council report on the grid, delivered to the White House in October 2010.

I was fortunate to serve on that council with a number of industry CEOs.

Resiliency requires proactive readiness for whatever may come our way. It includes robustness, the ability to minimize consequences in real time. The ability to restore essential services. The ability to adapt and learn.

Examples of the NIAC [National Infrastructure Advisory Council] team's recommendations include: one, a national response plan that clarifies the roles and responsibilities between industry and government; two, improving the sharing of actionable information by government regarding threats and vulnerabilities; three, cost recovery for security investments driven by national policy; and four, a strategy on spare equipment, with long lead times such as electric power transformers.

NERC is moving forward with a number of our own actions to complement our mandatory CIP [critical infrastructure protection] standards and provide enhanced resilience to the grid, including partnering with the Department of Energy and the National Institute of Standards and Technology to develop comprehensive cyber security risk management guides for the entire electric system, from the meter to the bulk power system.

Making actionable information available to the industry is a priority for NERC. We worked with DOD, DHS [the Department of Homeland Security] and other agencies in 2010 to issue high-quality alerts to the industry on the Aurora mitigation, the Stuxnet malware and VPN [virtual private network] tunneling vulnerability.

We are developing a North American cyber security exercise to prepare for and test a national response plan. In recent meetings at the USNORTHCOM [U.S. Northern Command] and the Pentagon, we have begun collaborating with DOD on assessing worst-case scenarios and developing case studies at critical military installations to ensure that essential requirements for national security are being addressed.

We are engaged with the DOE National Laboratories in opportunities to apply the expertise of the federal government in enhancing the cyber security of our grid.

In 2010, we started conducting onsite security sufficiency reviews at utilities, and we will continue that program in 2011. And we are working with vendors and industry to enhance—to demonstrate enhanced physical security of our systems.

The emerging challenges we face are difficult but not intractable. I believe we can and must take decisive actions through partnership between industry and government to meet these challenges. And I thank you, and look forward to your questions.

[The prepared statement of Mr. Cauley can be found in the Appendix on page 56.]

Mr. THORNBERRY. Thank you, sir. I appreciate it.

Mr. Nojeim.

STATEMENT OF GREGORY T. NOJEIM, SENIOR COUNSEL AND DIRECTOR, PROJECT ON FREEDOM, SECURITY AND TECHNOLOGY, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. NOJEIM. Thank you, Chairman Thornberry, Ranking Member Langevin, and members of the subcommittee.

Thanks for the opportunity to testify on behalf of the Center for Democracy and Technology about cyber security and the role of DOD.

CDT [the Center for Democracy and Technology] is a non-profit, non-partisan civil liberties organization dedicated to keeping the Internet open, innovative and free.

The United States faces significant cyber security threats. While the need to act is clear, it is essential that we take a nuanced incremental approach that recognizes distinct roles for DOD, the Department of Homeland Security, and the private sector. Generally speaking, DOD entities should be responsible for military systems, DHS for civilian government systems, and the private sector should monitor its own unclassified systems.

We ask that you keep a key distinction in mind: Policy toward government systems can be much more prescriptive than policy toward private systems. The characteristics that have made the Internet successful—openness, decentralization and user control—may be put at risk if heavy-handed cyber security measures are applied to all critical infrastructure. In the case of critical infrastructures, one size does not fit all.

When DHS and private sector efforts to secure civilian, government and private systems fall short, it is tempting to conclude that Cyber Command and NSA [the National Security Agency] should lead outside the dot-mil domain. But they operate in a culture of secrecy—for entirely legitimate reasons—that would hamper civilian cyber security efforts that depend on public trust and corporate participation.

Instead, expertise and resources of Cyber Command and NSA must be leveraged to help DHS with its cyber security mission.

More robust information sharing from the private sector to the government and vice versa is one way to leverage resources. But policymakers must proceed carefully to ensure that information sharing does not devolve into de facto surveillance through ongoing or routine disclosure of private communications to the government.

When he unveiled the White House Cyberspace Policy Review, President Obama correctly emphasized that the pursuit of cyber security must not include governmental monitoring of private sector networks or Internet traffic. That is one of the overriding civil liberties priorities in the cyber security arena.

Another is ensuring the free flow of information. Even in a cyber security emergency, empowering the government to shut down or limit Internet traffic over private systems could have unintended effects, including discouraging network operators from sharing cyber security information that they ought to share out of fear that that information would be used to shut them down. They know better than the government when elements of their systems need to be isolated.

Despite the value of anonymity on the Internet, some have proposed sweeping identification mandates, even a passport for using the Internet.

Identification and authentication will likely play a significant role in securing critical infrastructure. We don’t dispute that. However, they should be applied judiciously to specific high-value targets—like classified military networks—and to high-risk activities, and should allow for multiple identification solutions. Finally, you should resist proposals that would damage cyber security by making communications less secure. We are concerned about proposals to extend communications assistance for law enforcement design mandates to communications applications to facilitate electronic surveillance, as is being sought by the FBI. Because it could weaken communication security.

Privacy and security cannot be viewed as a zero-sum game. Measures intended to increase communication security need not threaten privacy and indeed can enhance it.

We look forward to working with the subcommittee to identify and promote these win-win measures.

[The prepared statement of Mr. Nojeim can be found in the Appendix on page 65.]

Mr. THORNBERRY. Great. Thank you.

I will look forward to the same thing.

I am going to reserve my questions and give other members have a chance.

And I would yield first five minutes to Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman.

And panel, thank you.

It is interesting, we have Dr. Pfleeger on one end and Dr. Nojeim on the other, because many of the things that Dr. Pfleeger was proposing to do fly in the face of what Dr. Nojeim was saying in terms of some of the prescriptive things that would happen.

To follow up the Chairman's original comments about the analogy between a physical attack on America and the response that the federal government spoken, you know, it would have been the military, of course, but the federal government's response to that is pretty clear. Trying to look at those solutions in cyber, given that the cyber attack happens in the blink of an eye or less and the warnings aren't nearly as easy to discern obviously captures the problem we have.

Who out there among the think tank groups are proposing solutions to that? In other words each of you brought—maybe that was your mandate—brought narrow, focused solutions to the issues, but is there a group out there that is looking at the broader issue? How does it—you know, what is the federal government's role—DOD and NSA—with respect to the dot-mil and homeland security? And then nobody on everything else has Dr. Nojeim concerned. Is that a rational way to continue down this path?

Mr. NOJEIM. I don't think that anybody is out there proposing that there is a silver bullet. I think that most people who are engaged in this endeavor all recognize that there needs to be a number of incremental steps taken.

To the thought that there is a silver bullet I think flies in the face of the kinds of risks that we are facing. We are going to have to have a situation where industry and the government cooperate—and sometimes very closely—in order to deal with these risks.

We have suggested not that industry has to stand alone when those packets are coming toward them, but that there is a very strong role that the government can play in helping out. It includes information sharing. It includes the sharing of attack signatures that will help the private industry identify the attack as it comes in.

Mr. CONAWAY. And that is the sharing of information that Dr. Pfleeger was saying ought to be done on a real-time basis as opposed to ad hoc every once in a while. Am I understanding between those two comments?

Ms. PFLEEGER. I don't think it necessarily has to be real time, but it has to be regular. As the threats change——

Mr. CONAWAY. Okay.

Ms. PFLEEGER [continuing]. We need to know what the changes look like.

Mr. CONAWAY. Not trying to put words in your mouth, but is that—do I understand what you just said in relation to what her comment was in terms of one of the solutions is to have a better way to gather the scope of the problem on a regular basis as opposed to an ad hoc basis?

Mr. NOJEIM. Oh, no. We agree that there has to be——

Mr. CONAWAY. Okay.

Mr. NOJEIM [continuing]. A lot of information sharing and that is——

Mr. CONAWAY. How you put that in place, that "requirement" in place without terrifying folks about your other comments that we are taking over the Internet, you know, all the other things. That Internet nonsense is going out there right now as a result of some of the comments the President made and misinterpretation of those. How do we bridge that gap?

Mr. NOJEIM. I don't think you have to have a world where communications traffic that is private-to-private traffic and is coming over an Internet backbone has to be shared with the government. I don't think that anybody's proposing that world.

I think what we do need is a world where if a private industry sees anomalies, they can share information about those anomalies with government agencies that need to act on them and that that can happen quickly, and it can happen in near real-time.

Mr. CONAWAY. Let me—before my time runs out, Mr. Cauley, help me understand the scope of your national test on the security exercise. Is that just with respect to the electricity grid that you are talking about doing, or is that broader infrastructure than just electricity?

Mr. CAULEY. Congressman, this year the exercise will be fairly limited in scope. We are looking to pull in all the key players in the industry in terms of participating in the exercise and demonstrate the communications and emergency scenarios that we might see. We do have interfaces with Homeland Security, DOD and Department of Energy and others, who will participate in that exercise.

One of the challenges that we are looking to try to resolve during such an emergency is what are the relationships between industry and government and how do we crystallize what those relationships should be and who is in charge and how that works. So we are hoping this exercise in the fall of this year will help answer and maybe clarify what additional questions need to be answered with that regard.

Mr. CONAWAY. Thank you, Mr. Chairman. Yield back.

Mr. THORNBERRY. Thank the gentleman.

The ranking member.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, to the panel, thank you for your testimony today. All this is, obviously, fascinating and very important work.

If I could, Mr. Cauley, I would like to start with you. First of all, thank you for refreshing my memory, just the record mentioning that you are new on the job at NERC as the chair. Thank you for the wealth of experience you bring to the job. And I certainly look forward to working with you in that role.

Let me ask. You touched on some of the things in your testimony about what has changed since 2007, but for the point about conversation, would you highlight against some of those things that have changed over the last few years?

And I still am of the opinion that NERC and FERC [the Federal Energy Regulatory Commission] really still lack the authority to direct all power utilities to follow the cyber security regulations, so I would like you to touch on that as well. And actually, how do you know that the government's guidance is being followed or that we are actually secure?

Mr. CAULEY. Thank you, Ranking Member Langevin.

The industry has evolved quite a bit. As you know, the issue of cyber and physical security is relatively new to the industry compared to the 100-year history of the industry.

I have had the opportunity in the past year to go out and meet a number of CEOs in most of the industry, and I believe that the awareness and the commitment is there that perhaps may not have been there before, but certainly has been elevated. And I feel we have the support of the industry.

The standards that we had have been in transition, so I think we have evolved and improved standards. We just recently approved a new standard with a bright line criteria in terms of what are the critical assets that need to be covered by our cyber security standards. And we are in the process of adopting NIST [National Institute of Standards and Technology] controls into our standards, and that work continues.

I believe at this point that the Federal Energy Regulatory Commission has full and adequate authority to direct us to do any additional standards or modifications to the standards that would be required to protect the security of the grid. In terms of——

Mr. LANGEVIN. Would you agree, though, that FERC doesn't have the kind of robust authority that, say, the Nuclear Regulatory Commission has when dealing with threats or things that need to be directed is done?

Mr. CAULEY. Yes, sir. I was going to get to the point where I think there is—there may be a gap, I think, that does exist. So in addition to the standards, we have the ability to put actionable information to the industry. We have improved that process.

So where I think we have a gap, a very narrow gap that has been narrowed with their activities over the last couple of years, is in an emergency situation, if there is an imminent threat to the grid, at this point we have the ability to put that information out, but not to produce a mandatory requirement in a short amount of time.

In that arena I do support expanded authorities for the federal government. It could be FERC or it could be another agency, but I believe there is an opportunity as an authority I would like to have. For an emergency imminent threat to the grid, action must be taken.

I would caution, however, that the grid is a very complex machine. Ordering certain actions can have adverse consequences, even to the point of taking down the grid, so that involving NERC in that process and putting the directive in the form of a conservative action, conservative position, but not telling operators how to operate the system, would be most effective.

Mr. LANGEVIN. Thank you. And I would certainly look forward to working with you on closing that gap.

Mr. Chairman, if you could, would you—does NERC work right now with DOD, identifying threats to the electric infrastructure critical to our military readiness? I know you talked—said that in your testimony, for the purpose of the record, would you expand on that?

Mr. CAULEY. Yes, Ranking Member Langevin. We have just begun that recently, and we are in the process of ramping that up.

The first thing we are going to do is look to develop a design basis scenario. I think the industry has a perspective of what are the worst-case scenarios that can happen from their own risk management perspective, but when we look at national threats, obviously those risks tend to be more widespread and potentially more devastating.

So we are in the process of beginning to develop a national cyber and physical security attack on the grid and what is the worst-case scenario that we could work from. That will drive things like the extent of our emergency plans, do we need spare equipment, and those kinds of questions.

The second piece, just to be brief, is working on an installation-by-installation basis in terms of, are there adequate redundancies and procedures in place to ensure that each critical installation will have power supply and, if it is taken out, that we would have the capability to restore power very quickly.

Mr. LANGEVIN. Okay. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. Thank the gentleman.

Mr. Gibson.

Mr. GIBSON. Thank you, Mr. Chairman.

And appreciate the panel today. Very informative testimony right across the board.

I actually want to pursue the experimentation question just a little bit further. So I am understanding that this is the first time, sir, that your organization is participating in this type of exercise in 2011. Yes, sir?

Mr. CAULEY. If you are referring to the national exercise——

Mr. GIBSON. Yes, secure grid exercise.

Mr. CAULEY. We have done training and exercises historically in preparations for hurricanes and earthquakes and known types of risks. We have participated most recently in Cyber Storm III and the previous versions of Cyber Storm, so we have participated in exercises.

What we are proposing to do this year is to get—in our exercise is to get greater involvement by industry rather than a sampling of industry, and gauge our entire communications infrastructure. We have an ability to communicate with the operating companies directly, and rather than having a government-driven exercise, where we bring a few of them in, I want this to be industry-driven, where the government folks can participate with us.

Mr. GIBSON. I am trying to—where I am driving is I am trying to get an appreciation for just how secure our electrical grid is, and I am trying to get an understanding of the exercise that is going to try to draw conclusions about that.

So you mentioned you are still drawing up the design for the exercise. What principles are you using to ensure your sampling geographically and with enough depth that you are going to be able to draw significant conclusions from the exercise?

Mr. CAULEY. Congressman Gibson, I think we are talking probably several different things. So in terms of the actual evolving security of the grid, I believe we are enhancing that continuously. We have standards for firewalls and protections and access controls and those kinds of things.

So the actual security is progressing in terms of continuously improving. The challenge is, what is the worst thing that could happen? And we are in the process of working with Department of Defense to postulate some potential extreme events, like take down major cities, take down major oil refineries or military installations.

Those scenarios, we have not run those in the past, and we are developing those as new this year.

We currently have the ability to communicate directly and have robust communications with industry folks. But now with this new scale of a scenario we have not seen before we will test that and demonstrate our ability to meet that challenge.

Mr. GIBSON. And one final question on this same topic. So as private sector, as research and development is done on the possibility of moving beyond copper for transmission, are you comfortable that there is enough collaboration that you will be able to make assessments as far as security going forward?

Mr. CAULEY. We have very open dialogue with national labs and other agencies in government, that we are trying to take advantage of every technology that will be useful and practical and cost effective for implementing in the private sector.

Mr. GIBSON. Okay. Thank you.

I yield back.

Mr. THORNBERRY. Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman and Mr. Ranking Member. I commend you for holding this hearing and look forward to joining you in the hard work that will be necessary to secure the cyber domain.

There is an emerging consensus that we need to clear jurisdictional distinctions between military and civilian cyber security efforts. Just as the military does not police our streets, it should not police our civilian cyber infrastructure.

But we must ensure that the armed forces will have the necessary tools to prosecute and defend the country from cyber warfare.

One note on private sector regulation. As we draw these fine jurisdictional distractions, Congress should establish hard regulatory requirements, not just soft suggestions of voluntary security measures to ensure the security of our private sector technology infrastructure.

We do not merely recommend that airlines maintain the highest standards of safety and reliability. Likewise, we must not merely recommend that American industry implement state-of-the-art best practices to ensure cyber security. We must require it, and there should be penalties when those requirements are not heeded.

My first question I would ask each of our panelists, what is the first question, the essential question for determining whether any given cyber threat should be the purview of civilian or military cyber security authorities?

Ms. PFLEEGER. That is a difficult question to answer because the military often uses private sector networks to accomplish things. And the threats to national security can be economic, they could be espionage, they could be a variety of things.

So I am not sure that—I think it would be a case-by-case answer rather than a one-size-fits-all answer, which I think reinforces what Mr. Nojeim said, that there is no silver bullet for security. And it is very difficult, I think, to—I think you need to look at the threat models and use the threat models to decide when the military should step in and when it shouldn't.

Mr. JOHNSON. Thank you.

Mr. CAULEY. Congressman, first I would agree that mandatory requirements and enforceability are one element in establishing an adequate defense. And we have those standards and are looking to continue to improve those for the electric grid.

I think to answer your question directly, it is the responsibility of the asset and information owners to protect their assets and their information. And I think those are divided into government and private sector assets and information.

However, the reality is we are very much intertwined. Military bases and systems depend on electricity. So we are bound together not only in the information world, but also in the electric world.

So I think it is important to complement that clear line of responsibility and accountability for securing our own systems to make sure that our actions are also complementary and helpful to each other.

And so I think there are opportunities for the military to assist us in information awareness, and when we are under attack and maybe don't know it, and vice versa, for us to ensure we have done everything we can to provide reliable electric service.

Mr. NOJEIM. I agree with both of the other panelists.

I think that one thing to keep in mind is that you often won't know what precisely was the source of the threat, what was the source of the problem. So then it becomes difficult to say who is responsible to respond to that threat.

But you—I think it is easier to say that everybody should be securing their own systems or the systems for which they are responsible, and to add that, if I am securing my system and I learn about information that would help Mr. Cauley secure his system, I need to have a way to share it. And that is, I think, where a lot of productive work can be done.

Mr. JOHNSON. Thank you.

Mr. Nojeim, in the physical world there are clear differences of capability and role between civilian law enforcement and the armed forces. The military wields superior firepower, specializes in destruction instead of arrest or investigation, and is subject to less restrictive rules of engagement.

What are or should be the equivalent differences of role and capability between civilian and military cyber-security authorities?

Mr. NOJEIM. You know, some of the capabilities are going to have to be similar. So, for example, say the National Security Agency has the ability to distinguish which—what is an attack signature that could threaten—of malware that could threaten a communications system. That information is useful, not just to the NSA, not just to Cyber Command, not just to the Department of Homeland Security, but to many people who are trying to secure information systems.

The point that I am trying to get across is that while we talk about and I have talked about having distinct roles for each of these entities, we can maintain that distinction by relying on other activity that will help secure all networks better.

One of those activities is information sharing, which I have talked about, and another is the sharing of expertise. There may be expertise within the military and at the National Security Agency that would be helpful to the Department of Defense, and there is already a mechanism to allow for the sharing of some of that information.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentleman.

Mr. West.

Mr. WEST. Thank you, Mr. Chairman, and thank you, Mr. Ranking Member, for the panel being here today.

I think when we look at this 21st-century battlefield it is definitely different from what we encountered in the 20th century. And of course it is multi-dimensional, multi-spatial. And of course the cyber realm does bring some interesting challenges.

So my question, going back to my time in the military, we always had this thing called mission-essential vulnerable areas, and we always sat down and looked at what was our high-value target list, the things that we knew that we needed to protect from our adversaries and our enemies.

So my question is, in your assessment, what systems should be considered critical to national security, and under what framework should the government and the Department of Defense in particular provide for the security of private networks, both to those deemed critical to national security and to a wider user base?

I will open that up to the panel. And subject to your response, I will yield back to the Chairman.

Mr. CAULEY. Congressman, I would take this on from the perspective of the electric grid in relationship to military.

We have taken steps to identify what are the critical assets within the grid, and we have approved a standard requiring companies to identify those. Obviously, nuclear plants are essential. Large-generation, high-voltage transmission that serves as the backbone of the grid. Blackstart generation that allows us to reboot the system if it needs to be done. And our larger control center.

So we are in the process. We have required that. What that may not get to, however, is the relationship with security—the military installations, which as I mentioned, the initiative that we have started with DOD is to identify if there is, besides our own electric priorities, what are the priorities of the military that we need to take a look at as well.

And then at that point it becomes a decision between the electric company servicing that facility and the military base in terms of what additional steps would be needed.

I would add one more aspect that I hadn't had a chance to mention. There are going to be some actions and threats that are beyond the capability of the industry to cope with.

And an example, much has been said about a nuclear blast 400 kilometers in the sky creating an EMP [electromagnetic pulse] event that takes down the grid. And—suggesting we need to understand the relationship between government and industry in resolving issues. That is a poster child for that, because I think the industry would say that is a government issue, if we have a nuclear blast going off over our skies in the homeland. Obviously, we would be expected to take some actions in terms of protecting and hardening the grid. But those issues need to be worked out further.

Mr. WEST. Then the follow-on question is, do you think we have a clear line of delineation between the responsibilities of, you know, the government, DOD and the private sector?

Mr. CAULEY. No, sir, not to the extent needed for clarity of responsibility facing these new threats. I think the collaboration, consultation has been good, but I think it is based on ad hoc relationships and not clear lines of responsibility and authority.

Ms. PFLEEGER. I would like to use two examples to address your question. The first is there is a model that seems to be working that the Defense Department is already using called the "defense industrial base," where collaboratively the major contractors come together to share their cyber experiences and to share the things that they have done in order to address any kind of cyber problem.

That might be a good model for expanding in some way, and the roles there I think are fluid because I think collaboratively, the defense industrial base acts to help the Defense Department, but at the same time makes clear what their individual goals are as private enterprises.

The other thing is that I would encourage the Defense Department to think more about prevention, rather than reaction to cyber attacks. And let me use an example. I was at a meeting a couple of years ago where someone from DARPA [the Defense Advanced Research Projects Agency] was talking about funding a system where the whole, for example, the whole communications system in the U.S. could be viewed on one screen and you could watch as a cyber event unfolded that one part of the country goes down, then another, then another.

The problem with that example is that it might not have been a cyber attack. It might have been that all the phone companies are buying their switches from the same vendor. There is a flaw in the switches and they all happen to be going down because some system problem was percolating through the system.

So that is what I meant in my testimony about the difficulties of emergent behavior and the risks of making assumptions. And so it is very hard in those cases to decide not only what is going on, but what is the appropriate thing to do to react.

Therefore, I think it makes a lot more sense to look from a preventive point of view at things like our critical infrastructure and look at more diversity, look at redundancy, look at ways of making sure that if we do have some sort of attack, we can come back up quickly or at least in some manner that enables the Defense Department, as well as private enterprise, to function while we figure out what is really happening and apply fixes.

Mr. NOJEIM. I would just add that there is a list of critical infrastructure key resources, tier one, tier two lists. DHS has prepared it. It is based on assessments as to what would happen if these were destroyed or rendered inoperative; in terms of casualties, whether people would have to evacuate areas; what would be the damage to national security.

So there has already been a lot of thinking about what needs to be protected. We don't have to recreate the wheel on that score.

Mr. THORNBERRY. Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

Thank you all for being here. You provide a broad range, and that is appreciated.

I don't know whether you would feel prepared to answer this question specifically, but I am wondering about interagency collaboration, coordination. One of the things that we experienced here on the Armed Services Committee a number of years ago was sort of our shock that in fact, you know I guess I would say the Pentagon and the State Department didn't really talk to each other to the extent that they should, and that we really weren't looking at a whole-of-government approach, if you will.

Can you apply that to the issues that we are addressing here in terms of cyber security? How would you assess the extent to which that is kind of a working—I guess it is a work in progress in many ways—but where are we in that issue, to look upon how we best deal in an interagency way on this issue?

Ms. PFLEEGER. Well, there are some formal and some informal things going on. There was for a while an Infosec Research Council where different agencies funding cyber security research had representatives get together periodically and share what they were doing and coordinate.

There are more formal things like the Department of Commerce now has an Internet Policy Task Force that is looking across the government. But you are absolutely right that a lot more needs to be done. There needs to be a lot more regular interaction at high levels across the different——

Mrs. DAVIS. Any area particularly that you would seek to improve, specifically if we could focus on that?

Ms. PFLEEGER. Well, certainly discussions between Defense and Commerce and between Defense and State. Those are probably the two I would pick.

Mr. CAULEY. Congresswoman, with respect to the electric system, we have had very collegial consultation with a variety of agencies, and they are very helpful. I think if we are challenged it is just a confusion over leadership and the relationships between the different organizations, and the relationships between government and private sector.

So they are collegial. We are getting worked on. We are learning. They are learning from us. We are learning from them, but it is not clear what the delineation of responsibilities, who is in charge, those kinds of questions. We are making do with what we have today.

Mrs. DAVIS. Who is in charge, that is a big question. We got that, yes. Thank you.

Mr. Nojeim, do you want to comment on that as well——

Mr. NOJEIM. I would just say that there is some cooperation, some communication, and that it is starting to get better and it needs to go further.

Mrs. DAVIS. Can I just ask you a little bit about the labor force as it relates to this highly complex STEM [science, technology, engineering, and mathematics] area of education and science and technology. Clearly, we are not where we want to be generally in the country as it is in terms of encouraging young people to go into the field.

Can you assess sort of the labor force and those people who are migrating to these careers and to this area? And what we—what else—what should we be doing, even in terms of preparing our youngest children, I think, in having the ability to work in this area since we know that, as I know as I am just getting introduced to this topic and our concern that state actors make us very vulnerable. And we obviously need to be providing that expertise to our young people as well.

Any thoughts, ideas as far as the labor force?

Mr. CAULEY. Well, in the electric industry, we are seeing an influx of talent. I mean, I think it is pretty obvious that kids will go where the jobs are. We are seeing very high influx. And we are also focused on training. I think we do have a gap that we are working on which is to elevate the credentials, the professional credentials of our security—physical and cyber security folks.

So I think its major improvements in the last couple of years, lots of new talent coming in, but a long ways to go as well.

Mrs. DAVIS. Yes?

Ms. PFLEEGER. In many cases, the people who provide cyber security expertise don't do only that, especially in small businesses. And so we are having a workshop at the end of April at Georgia Tech to look at the demand, to help inform what the supply should look like. And we are inviting people from government and industry together to tell us what their demand looks like and what some of the problems are so that we can make some recommendations about what the supply activities should look like.

Mrs. DAVIS. Thank you.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Mr. Ryan.

Mr. RYAN. Thank you, Mr. Chairman.

I just have one question. One of the issues we have not just with—I am going to ask if it fits into the cyber strategy that we all should have as a country—is the issue of translating a lot of different languages. Is that an issue when we are talking about cyber security, where we have, whether they are state actors or a decentralized, you know, Al Qaeda-type, where these folks are working from a different language than the English language, and trying to attack our systems.

And, you know, is this an issue for us? Is this something that we need to be aware of? Because clearly, I know as far as the private sector goes, you are talking about Mandarin and Farsi and being able to have enough Americans able to speak these languages, to write and read in these languages for our corporate interests, as well as our governmental interests.

I just wondered as I am sitting here listening, is that something that we should be concerned about not having, on top of what Ms. Davis was just saying, the workforce capable of helping us address this problem?

I will let you answer and yield back the balance of my time when you are done.

Mr. CAULEY. Congressman, from an electric perspective, I don't view that as a priority at this time. For North America, all of our information exchange is done in English, including in Quebec where French is the language. But the electric grid operations are purely English.

So we treat anything that is not in English as suspect to start with. So it is not really an interpretation question for us. It hasn't come up to our attention at this point.

Mr. NOJEIM. I think at one level, bad code is bad code and it is not really a question of whether it is English language or Spanish or another language. I think that the issue about needing people to speak in multiple languages comes up mostly in terms of prosecuting wrongdoers and being able to understand what people are saying who are perpetrating the crimes.

Mr. RYAN. I know at one point we had an issue with a lot of the intelligence we were getting. We weren't able to translate a lot of the, you know, kind of prepared for attacks against us, we weren't able to do that. So I just want to throw that out there if that is something we need to continue to look at.

Mr. THORNBERRY. And that is still the case with a lot of intelligence we get. We don't have the resources to translate it, so I thank the gentleman. Dr. Pfleeger, you talked about incentives in your statement. It has been suggested to me that with proper incentives, we can elevate general cyber security that would take care of roughly 80 percent of the problems that are going through cyberspace. Do you think that is about right?

Ms. PFLEEGER. Well, I don't know if it is 70 percent, 80 percent. What I—two days ago, Arbor Networks revealed the results of a survey that they did of network engineers. And the top problem that the network engineers talked about was non-technical factors being one of the most significant obstacles to reducing mitigation time.

A lot of that has to do with there being a lack of incentives for the people maintaining the networks to pay more attention to security; the lack of users to pay more attention to security. And so because a lot of these non-technical problems loom large, that 80 percent number is probably close.

I mean, if you look at things like the causes of all a lot of typical problems, we see the same things over and over again. People don't change things from the default settings. They don't understand how to install security software.

If there were incentives to encourage people to do the right thing, what I called in my testimony good hygiene, won't completely solve the problem, but it could eliminate a lot of these things that we see that recur that shouldn't be happening anymore. We should know better by now.

Mr. THORNBERRY. Do you know of any organization that has actually run the numbers, by which I mean to say this incentive for this tax provision or this, you know, whatever it is, will have this consequence in the real world, because businesses are calculating cost-benefit every day. How much is it going to cost? What is the benefit I get? And that cost-benefit has to line up for them to take additional actions. Has anybody run the numbers to kind of get more specifics on it?

Ms. PFLEEGER. There are some researchers who have done some economic models that suggest which incentives might be the most effective, but I haven't seen a lot that use real-world numbers, in part because it is hard to get good data.

Mr. THORNBERRY. Yes.

Ms. PFLEEGER. So there are some first steps, but it would be really helpful if business would work with some of the modelers to—so that the models reflect the realities of the business tradeoffs.

Mr. THORNBERRY. Okay.

Mr. Cauley, especially in your written statement, you made reference to the fact that private industry is always going to be at least a step behind in identifying some of the most sophisticated threats that go through cyberspace.

I mean, just assume, if you will, that you can take care of 80 percent by good hygiene, we still have 20 percent that are the more sophisticated, difficult threats to deal with. And so from what you said earlier today, I take it in that area you think there needs to be more government assistance of some sort for that kind of upper tier.

Mr. CAULEY. Yes, Mr. Chairman. That is why I think we need a dual strategy. So the Ranking Member Langevin has suggested we need firmer regulations and standards, and I agree with that because it provides a baseline of the expected mandatory requirements.

But facing a dynamic, ever-evolving adversary, sitting still with fixed barriers is going to be very difficult. So having a robust relationship with the government intelligence agencies, which we are beginning to develop to take quick information and be able to turn it into actions that the industry can take, is essential.

So let's treat it like it is a dynamic, ongoing war, and it is not a fence put around the systems. And I think that is where we need the help from the federal government.

Mr. THORNBERRY. Let me ask you this. There has been lots of talk about a smart grid. To me that indicates that there are more access points on the grid to the Internet. Does that not increase our vulnerability—potential vulnerability of the electricity grid?

Mr. CAULEY. Mr. Chairman, it does create—introduce additional risks, additional entry points. And it is incumbent upon the industry and government, I think, in partnership to work out a sufficient set of security requirements for a smart grid and also for the vendors to deliver devices and systems that build in the security as a major objective from the start, not as an add-on later down the road.

Mr. THORNBERRY. Mr. Nojeim, I think Mr. Cauley a while ago kind of used the EMP example as a big, catastrophic sort of event that would require government direct intervention.

And I guess what I am wondering with you is do you—set EMP aside—what do you think there could be a situation where the cyber event is of such a magnitude as to overwhelm, perhaps, private ability to deal with it and that direct government action would be appropriate?

Or, as I think you have kind of indicated in your testimony, is it always—as far as direct responsibility, it is DOD for DOD, DHS for dot-gov and all of dot-com is on its own?

Mr. NOJEIM. So I just—if I gave the impression that all of dot-com is on its own, I didn't mean to do that, because what I did say in the testimony at least a few times were some measures that ought to be taken to help dot-com defend itself.

As for a catastrophic event that the private person couldn't deal with, I would need to just talk a little bit more and understand a little bit more about what that event would be. So, for example, some people have said that maybe the government ought to have authority to order the shutdown of Internet traffic to a critical infrastructure system.

Well, see, that authority, as you think that through, would only be exercised when the person who owns or operates the system thinks that it ought not to be shut down. And they have strong incentive to protect their system. They have a strong incentive to isolate their system when it is in danger, and they do that right now.

I think the question we have to ask is whether the government would have superior information that would inform that decision. And if so, that is kind of information ought to be shared.

And we also ought to ask other questions about what incentives that kind of authority would create. Would the owner operator of that system be willing to share information that they ought to share what they know that that information could be used to shut them down? Would they be more hesitant to shut down on their own when they think they ought to, because they are waiting to be ordered to shut down by the government, knowing that with the order will come a limitation of liability?

So I think we have to think these things through and maybe game out some scenarios before we make blanket decisions.

Mr. THORNBERRY. Okay. Let me ask one other thing, and then I will yield to the ranking member and others who may have questions.

But as I understand what you have said, you think there is an appropriate role for government to share with private industry information it receives about signatures and malicious attacks going on in cyberspace as long as it is the private entity that deals with it, that takes direct action of some sort.

Mr. NOJEIM. Yes. Yes.

Mr. THORNBERRY. And even though, obviously, if the government were to share some information with, say, a telecommunications carrier, the government will have to expect that some information is kept classified, potentially.

Mr. NOJEIM. And the government should expect and should help the telecommunications carrier have people on staff who can handle classified information.

Mr. THORNBERRY. Certainly.

Mr. NOJEIM. And if there is a gap there——

Mr. THORNBERRY. Absolutely.

Mr. NOJEIM [continuing]. And the right ones don't have the right clear cleared people, that is a place where the committee ought to pay particular——

Mr. THORNBERRY. Well, DOD deals with defense contractors——

Mr. NOJEIM. All the time.

Mr. THORNBERRY [continuing]. All the time in huge numbers, so, yes, I think that is a fair point.

Ranking member.

Mr. LANGEVIN. Thank you, Mr. Chairman.

To continue to explore this role of proper balance of authorities and such, particularly in time of crisis—and this is really for the entire panel—you know, do you think they DOD's role should be in specifically protecting not just our power systems, but other critical infrastructure, such as our financial institutions or communications sector?

Should there be any new structures set up to increase their coordination with the Department of Homeland Security, for example?

Mr. NOJEIM. I think there are some structures already. And again, when we think about role of DOD when it comes to securing private systems, it should be in a supportive role and that, for example, it should be supporting the efforts of the Department of Homeland Security to work with those private entities to secure their systems.

And Cyber Command and NSA are going to have information and expertise that will be useful. And the important thing is to loose it and to access it and together to DHS and to these other entities so they can do a better job.

Mr. CAULEY. I would answer that question. I think there is—I have seen evidence of good coordination between the Department of Defense and Homeland Security, but I will repeat my earlier comment that working to try to resolve electric industry issues related to cyber, it is a community of agencies.

It is not clear, you know, where all the responsibilities lie or where the authorities are, but we try to work with everybody.

I think there is an interesting set of questions here in terms of what DOD should be authorized to do in the state of an emergency. And I really wouldn't rule out—I sympathize with my fellow panelist's comment that it becomes very, very scary if a government agency can take an action that would alter the controls of the power grid, because it is just a scary thought. It could have unintended consequences.

But I can conceive of extreme denial of service attacks on the Internet or sort of a major cyber concurrent attack on the entire country, where intervention by DOD might be beneficial just to stop the bleeding in the initial minutes and hours. And I think that would merit some more dialogue in terms of what that would look like, but overall I think the industry needs the information to act under most circumstances.

Ms. PFLEEGER. I suggest that the DOD consider again the threat models and try to work collaboratively in advance with providers of the key infrastructure, perhaps by giving them scenarios. So the DOD might suggest, for instance, that the electric grid have the capability to do a handful of things that would be useful to both the grid and the Defense Department, if there were an attack on the grid.

I think that kind of in—advance, preventive set of measures might be more effective than just having a blanket ability to—for the DOD to take over something that it is not used to running.

Mr. LANGEVIN. Let me turn to something else. You know, there is a debate around, you know, what constitutes cyber warfare, what constitutes a cyber attack, if you will, versus defense. You know, and basically how involved should our military be in cyber security when you look at, for example, computer network operations by DOD. Much of this debate focuses around—what constitutes "warfare," you know.

Could you provide a definition to us about what cyber warfare is and what it looks like, and what the appropriate response should be?

Mr. CAULEY. Ranking Member Langevin, I have seen enough in the last few months—just in my visits with NORTHCOM and the Pentagon—to understand that the Department of Defense has a much richer understanding of the ongoing cyber warfare than we have in the private sector.

So I think anything that can be done to not just keep that information internal as we know what is going on in the cyber warfare arena, but how can we help industry understand the information they need to know to—to be aware of what is going on.

I myself have a top secret clearance—been to some of the briefings. I have understood more than I had in the past. And it is serious stuff going on. And I think we need to be able to share that with industry in a timely fashion.

The tendency is, because it is a war, to keep it inside the military and not share it. And I think we have to figure out how we overcome that a bit.

Mr. LANGEVIN. Well, I yield back.

Mr. THORNBERRY. Dr. Pfleeger, one of the challenges the government always faces is how to have a role that does not distort the market in some way. And I am thinking about especially research in this area.

Obviously, the Microsoft and the Dells of the world are doing lots of research about next phases of computing that can be more secure. Do you have suggestions as to the government's role in funding specific kinds of research that would be complementary but not displace the role that private industry plays?

Ms. PFLEEGER. I think there are already a lot of activities coordinating what the private sector is doing with what our universities should be doing and what the government should be sponsoring.

Both within the DOD and the Department of Homeland Security they have lists of their key topics that they try to fund.

I think the place where there is room for improvement is that often the focus is on the technology alone and not on how people use the technology or perceive the technology. And so I think that is an opportunity for improving not just the kinds of technology that we are producing to make things more secure, but improving the technology transfer, improving the eagerness with which users view the security. If they could view it more as an enabler than as an obstacle, I think that would make a huge difference.

So it isn't always what the technologists like to get funded to look at, but in fact, technology that isn't used properly or isn't used at all is fairly worthless.

Mr. THORNBERRY. Let me also give you a chance to weigh in if you would like on this question about emergency powers. Because I know it has been very controversial in some of the Senate bills about to what extent a government ought to have ability to take emergency actions. And you have heard a little bit of it addressed here.

Do you have views on that?

Ms. PFLEEGER. I don't really have a view. I have looked at some of the issues. But I am not a lawyer. I am not a historian. I am not sure it would be appropriate for me to make a judgment.

Mr. THORNBERRY. I appreciate it.

Yes, gentleman from Texas.

Mr. CONAWAY. It occurred to me, that as you are looking at this new cloud concept where everything is out that—the things that we are talking about today—before that—in other words, all of that innovation which creates greater accesses and from anywhere you want all your data is out there.

Does the stuff we talked about today really contemplate that at all?

Ms. PFLEEGER. Do you mean—if I understand you, you are asking whether the kinds of recommendations that we made in our testimony——

Mr. CONAWAY [continuing]. Yes, just the state of play, is the state of art for—does the users out there remotely understand the risks they take, that you are relying on private entities to protect all of that?

It just occurred to me that we fight this fight right now where most everybody's stuff was on a laptop and you had a direct access line. But now with this—the new innovations and the continued improvements and everything, do we really contemplate—are these recommendations getting as far ahead as what that is ahead of the normal way people understand what is going on?

Ms. PFLEEGER. Well, I think the cloud computing is a good example of misaligned incentives. Because a lot of people—a lot of organizations are choosing to use the cloud because it is cheaper without being aware, as you point out, of the risks that they are taking.

And so I think a lot of these questions are being raised. But there aren't a lot of good answers yet.

Mr. NOJEIM. I think that it is a double-edged sword. And you could have cloud providers that are better at security than the individual user is on his or her laptop. So maybe if more users demand more security, we will get better security as a result of migration to the cloud instead of worse security.

Mr. CONAWAY. But is the driver—is the free market system robust enough to drive those kinds of things without the users knowing it and/or appreciating it——

Mr. NOJEIM. I think it depends on the user. There are some users that are large corporations that are moving to the cloud and they are asking these questions——

Mr. CONAWAY. They will drag along the protections for all those folks——

Mr. NOJEIM. They are going to drag along the protections for—you know, obviously, they are interested in protecting their own data. I think the issue is whether the practices become such that they become more a standard at a higher level as a result of the demands of industry. As it moves toward the cloud it would filter down and help consumers.

Mr. CONAWAY. Okay.

Thank you, Mr. Chairman. Appreciate that.

Mr. THORNBERRY. Let me just—I have been trying to take notes and see if I can summarize, at least, some areas where it seems to me you all are pretty well in agreement.

One is that the government does need to take some action. That continuing to let things drift along as—that may be a little—continuing as we are without some additional action would be a mistake.

Secondly, that there needs to be some further action in the form of incentives, regulations to encourage a general—or to mandate a general increase in cyber security.

Third, that at a minimum, the Department of Defense should ensure that the appropriate entities in the private sector have access to more of the information that the Department of Defense has in order to protect those private networks better.

So have I—does anybody disagree, I guess, with at least that starting point?

Now, you all have to say something. They can't——

Mr. NOJEIM. I think that is a good starting point. I think that, you know, people are going to say, "Well, I didn't call for more regulation," or this or that.

But——

Mr. THORNBERRY. Yes, yes.

Mr. NOJEIM [continuing]. I think that, you know, when we look at incentives, we look at accessing information that the government has and spreading that out, I think that there is a general consensus about that.

Mr. THORNBERRY. And you are okay with increase incentives and considering, at least, looking at regulation of certain sectors that are already regulated, at least, as something——

Mr. NOJEIM. Yes.

And as I said, we think that different sectors are going to be subject to different rules.

Mr. THORNBERRY. Yes. Yes.

Mr. CAULEY. Mr. Chairman, I would generally agree, as well with a couple of nuances. I think there does need to be clarity within the various agencies in the government in terms of roles and responsibilities, and who do we work with as private sector.

I think in terms of the mandates to industry, my sense is we have—in the electric side, we have addressed that mostly through existing structures through the Federal Energy Regulatory Commission and our ability to do mandatory standards.

I did point out a gap, I thought, in emergency, in an immediate threat—do we need a mandate and action?

I think there is a danger of further escalating the mandatory compliance directive aspect because we may drive the electric industry to sort of a common plateau of mandated regulations. And I am trying to get them to fight the dynamic warfare in cyber—so I think we can over-regulate when we have a solid foundation. So I just want to make that distinction.

Mr. THORNBERRY. And that is a fair point and an important amplification, I think.

Ms. PFLEEGER. I also agree that it is a good summary.

I think, in addition, the government could—I think we would probably all agree that the government could encourage private sector initiatives that already are good behavior. There already are examples of private enterprise making data public, collaborating in various ways. And so making that more visible and providing incentives in that way might be helpful.

Mr. THORNBERRY. Okay.

We may want to pursue—I have some other questions on that line that we may want to pursue with you.

Anyway, thank you all very much for being here. I appreciate your testimony and the time it took to prepare it, and for your being here.

With that, the hearing stands adjourned.

[Whereupon, at 12:59 p.m., the subcommittee was adjourned.]

APPENDIX

FEBRUARY 11, 2011

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 11, 2011

Statement of Chairman Mac Thornberry (R–Texas)
House Armed Services Subcommittee on Emerging Threats and Capabilities
Hearing on
What Should the Department of Defense's Role in Cyber Be?
February 11, 2011

One of the first things that one notices is that the name of the subcommittee has changed this year to better match what our charge is. We are to look out into the future and help see that the United States is prepared to deal with those national security challenges that are still emerging—those that we are still learning about, such as terrorism and cyber warfare.

We are also charged with nurturing emerging capabilities that can meet those and other threats. The jurisdiction has been clarified so that we can better focus on cyber and other issues.

Any emerging threat presents new challenges on policy, legal authority, budgeting, as we have witnessed, for example, since 9/11. Today, we want to start by asking a fairly basic but important question: What is the role of the Department of Defense in defending the country in cyberspace?

If a formation of planes or hostile-acting ships came barreling toward a factory or refinery in the U.S., we know pretty well what we expect the military to do. They may try to identify who they are and what they intend. They may try to divert them or shoot them down, but the bottom line is that we expect our military to protect us from threats we cannot handle on our own.

But what do we expect—or should we expect—if a bunch of malicious, or potentially malicious, packets come barreling toward that same factory or facility in cyberspace? And then the question will be whether the Department of Defense or the federal government is able and is authorized to do what we expect.

We do not expect definitive answers that everyone will agree with today, but we need to be serious and diligent about pursuing answers because the threat is serious—it is growing in numbers and in sophistication, and our vulnerability is growing because our dependence on cyber is growing in just about every aspect of our lives.

Yesterday, at an Intelligence Committee hearing I asked DNI Clapper, FBI Director Mueller, and CIA Director Panetta how serious a threat was posed to our country's security in cyberspace. Each of them said it was very serious. In fact, Clapper testified that "The threat is increasing in scope and scale, and its impact is difficult to overstate."

Cyber is a new domain of vandalism, crime, espionage, and, yes, warfare, but we are not very well equipped to deal with any of those challenges. As we look for solutions, we want to be smart, careful and true to our values, but we need to act to improve our security.

Statement of Ranking Member James R. Langevin (D–Rhode Island)
House Armed Services Subcommittee on Emerging Threats and Capabilities
Hearing on
What Should the Department of Defense's Role in Cyber Be?
February 11, 2011

Thank you, Mr. Chairman. As this is our subcommittee's first hearing of the 112th Congress, I just wanted to take a moment to congratulate you on your Chairmanship and to say that I am very much looking forward to working with you. We have enjoyed a productive partnership in the past, and I know it will continue with our work on this subcommittee.

In 2007, as chair of the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, I conducted a detailed and thorough examination of cyber threats to our power grid after tests conducted at Idaho National Labs, known as Aurora, became public.

At that time, industry representatives from NERC misled or were inaccurate in their testimony to the Homeland Security Committee about their efforts to address these threats in the private sector. We called them on it and they retracted their statements, but the experience illustrates how difficult it can be to require and ensure security when it comes to critical infrastructure.

Since then, threats to our critical infrastructure have only grown, with news reports suggesting that there is interest by malicious actors in exploiting vulnerabilities in the U.S. power grid and other critical infrastructure.

Federal agencies have taken steps to reduce these vulnerabilities, but I am afraid that many in industry – and in government -- still fail to appreciate the urgency of this threat. Since I began working on this issue, I have been disappointed by the overall lack of serious response and commitment to this issue and I believe America is still vulnerable to a cyber attack against the electric grid that would cause severe damage to not only our critical infrastructure, but also our economy and the welfare of our citizens.

Because of this concern, last Congress I posed this question to the heads for cybersecurity of all our military services: If our civilian power systems are vulnerable, what is being done to protect our numerous military bases that rely on them to operate? The answers were disturbing, but not surprising. Vice Adm. Barry McCullough, head of the Navy's 10th Fleet, testified that, "These systems … are very vulnerable to attack," noting that much of the power and water systems for our military bases are served by single sources and have only "very limited" backup capabilities. With an attack on a power station potentially requiring weeks or even months to recover from, our bases could face serious problems maintaining operational status.

A recent report from the Department of Energy's Inspector General found that despite years of concern and hand-wringing by those who are aware of the threats, not much has been done to increase protection for these civilian systems.

The report faults both federal regulators for not implementing the adequate cybersecurity standards.

But if you ask industry you will find out that there is no actual requirement to do what the government wants. The regulators don't have any actual ability to regulate when they see a problem, despite being fully aware of the tremendous risks that face our nation.

If everyone is aware of the threat, both DOD and our civilian power sector, it appears that the tragedy of the commons has ruled and that no one has been willing or able to address it.

At the House Intelligence's annual open meeting yesterday, Leon Panetta testified that cyber threats to our critical infrastructure had the potential to be the next Pearl Harbor. I agree and remain unconvinced that we have the abilities or the authorities to stop a large scale cyber attack.

To this end, last year, I introduced legislation to coordinate our national cybersecurity policies for the protection of our federal networks as well as our critical infrastructure.

While we had success with an amendment in the House defense authorization measure, we were forced to remove the language during conference.

I look forward to working with Chairman Thornberry, to move forward again this year and finally begin to address these critical vulnerabilities.

Today I am anxious to hear from our panel, especially Mr. Cauley from NERC, and ask what has changed since 2007? Are we still as vulnerable today then we were then? I believe the answer is yes.

I fear that little has changed other than the acceleration of the threat and the growth of our vulnerability.

Thank you Mr. Chairman. I look forward to hearing from our witnesses.

What Should the Department of Defense's Role in Cyber Be?

Testimony to House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, 11 February 2011

Shari Lawrence Pfleeger
Director of Research, Institute for Information Infrastructure Protection
Dartmouth College, Hanover, New Hampshire

Many thanks to the Subcommittee for inviting me to address these important questions. I am the Director of Research for the Institute for Information Infrastructure Protection, at Dartmouth College. The I3P is a consortium of 27 American universities, national laboratories, and non-profits focused on tackling problems in cyber security, dependability, safety and reliability. However, my opinions today are my own, not the I3P's, Dartmouth College's, nor my sponsors'.

I have organized my comments so that they address the three important questions posed by the Subcommittee's invitation to me.

What are the significant challenges facing the private sector, federal government and Defense Department in preparing for the defense of the nation's cyber infrastructure?

- **Diverse and distributed ownership.** Much of the nation's critical cyber infrastructure is privately owned, and the federal government, including the Defense Department, requires its uses in providing critical functions and services to the American public. For this reason, private enterprise must recognize its responsibility in providing secure and resilient infrastructure components. The government plays an essential role in encouraging or requiring private enterprise to find solutions that permit the nation's economic and social engines to function. However, traditional approaches such as service level agreements, reliability standards, and problem reporting are made more difficult by the diverse and distributed ownership of the cyber infrastructure. Moreover, the cyber infrastructure is constructed of many parts that were not originally designed to provide critical infrastructure capabilities; because many of the security-related parts are not the primary money-makers for their providers, there is often little incentive for the providers to put security concerns above functionality provision.
- **Appeal as a criminal tool.** Many criminals use the cyber infrastructure as a tool to perpetrate their crimes. This usage enables criminals to act more broadly, more quickly, and with more anonymity than with other technologies. It is important to address the increase in cyber crime and cyber attack without restricting the far-more-common legal uses of the cyber infrastructure.
- **Difficulty in quickly identifying and reacting to emergent behavior.** Cyber problems are usually emergent behaviors with high degrees of uncertainty about both cause and extent of effect. Consequently, the time between recognizing an abnormality,

understanding cause and effect, and selecting an appropriate reaction can sometimes be quite long. And there are significant risks in acting with insufficient information. The large service providers can often act quickly to spot and stop aberrant behavior, especially when a disruption in service or function is temporary and non-critical. But when the aberrant behavior's cause is not certain and involves possible responses with life-threatening or international diplomatic repercussions, decision-makers must take far more care in reducing the uncertainty surrounding cause and effect.

What policy, legal, economic and technical challenges are critical?

- **Misaligned incentives**. Economics and behavioral science provide numerous examples of misaligned cyber security incentives. (See van Eeten and Bauer, 2008 for a summary.) For instance, an organization that chooses not to act securely can nevertheless be protected by the secure actions of others. (This phenomenon is called "herd immunity," where someone is protected when enough others keep the level of "infection" down, or "free riding," where investments by others allow someone without investment to benefit, too.) Similarly, many organizations underinvest in cyber security: they take no up-front preventive or mitigative measures, preferring instead to deal with cyber attacks when they happen, and expending resources to clean up the resulting mess. (Rowe and Gallaher 2006) Indeed, Kunreuther and Heal (2003) point out that when one organization takes protective measures, those steps can actually discourage others from making security investments. These misaligned incentives sometimes result in good business decisions that are at the same time very bad security decisions. And the bad outcomes do not always affect the organization behaving badly, or not for very long. For example, the Defense Department may experience a breach of personal information about its soldiers, perhaps due to a cyber security failure. The impact is felt by the soldiers and their families; the breach may not cost the Defense Department much to remedy, and the long-term impact to recruitment and solider effectiveness may be negligible. Similar examples of short-term effect to reputation and stock price are documented in the cyber security economics literature.
- **The need for diversity.** Many researchers and practitioners have argued that technological diversity leads to more secure products and networks, (Geer et al. 2003) and several studies (for example, Danezis and Anderson 2005) suggest that systems composed of diverse resources perform better than those whose nodes have the same resource mix. However, for economic reasons (especially in terms of the cost of maintenance and support), organizations often prefer technological uniformity. Anderson and Moore (2008) point out how externalities such as market dominance and access to applications reduce diversity. Moreover, it is more difficult to assure diversity than it would seem. Knight and Leveson (1986) demonstrated that attempts at diverse design are often dashed because of commonality in the way we train our software engineers. Other diversity failures can emerge by chance, when lack of knowledge, system complexity,

and business confidentiality lead to architectures with unintended dependencies and unexpected points of failure.

- **Perceived lack of security choices compatible with organizational culture and goals.** Too often, decision-makers view security as an inhibitor of creativity and productivity rather than as an enabler. For example, my profile of a large, multi-national corporation under sustained cyber attack revealed that the corporate president refused to remove administrative privileges from all corporate computers for fear that it would inhibit employees' computational flexibility. (Pfleeger 2010) Other studies show similar problems, with practitioners disabling or avoiding security in order to "get their jobs done." (See Sasse 2004 for a survey of these problems.)

What should the government do to address these challenges?

- **Address cyber crime and cyber attacks the way other unwelcome behaviors are addressed.** The government should incentivize or require better breach, fraud and abuse reporting, much as the Federal Trade Commission and the Food and Drug Administration track consumer problems and adverse consequences. Similarly, data about the nature and number of cyber attacks should be reported consistently each year, so that sensible trend data can form the basis for effective preventive and mitigative actions. Currently, almost all states require breach reporting when personal information is revealed—a good first step at capturing much-needed data. Other countries, such as Britain and France, have mandatory public reporting of bank fraud by crime method; efforts could be instituted here in the U.S. by extending existing criminal statutes to include cyber crimes. Our current reliance on convenience surveys for information about cyber attack trends can be misleading; more careful sampling and more consistent solicitation of data are essential. Early attempts by the Bureau of Justice Statistics at capturing cyber crime data on a large scale with a careful sampling scheme (see Rantala, 2008) had significant drawbacks, as documented by Cook and Pfleeger (2010). It may be more useful to capture data in various ways for various purposes, but doing so consistently over the years so that trends can be analyzed; some of the common terminology, such as the CVE (common vulnerabilities and exposures) list, can be useful in this regard. Good cyber economic models, informed by these representative, consistent data, offer the opportunity to improve cyber security investments and our general understanding of cyber risk relative to other kinds of risk. (Rue and Pfleeger, 2009)
- **Extend liability statutes to cover cyber technology**, so that the creators and maintainers of cyber technology—just like other technology providers—are forced to take responsibility for its failure. The situation now in cyber is similar to that of automobiles in the 1960s. When a lack of car safety was made more visible, the government responded by making automobile companies more liable for their unsafe practices and products. And as with automobiles, a combination of manufacturer liability and economic

constructs (such as insurance) could encourage more secure cyber product design and implementation.

- **Insist on good systems engineering.** The government is a significant buyer of cyber technology, and its purchasing power can be put to use in two important ways. First, by keeping track of cyber-related failures (security and otherwise), the government can refuse to continue to deal with system providers whose products and services are demonstrably insecure, unsafe or undependable. The data gathered in this process have another purpose: they can inform subsequent requirements selection, design decisions, and testing strategies, so that errors made in earlier products are less likely to occur in later ones. Second, the government can insist that critical systems, not just software, must be accompanied by solid, up-to-date formal arguments describing why the systems are secure and dependable. Such arguments are used in other domains, such as nuclear power plant safety, and can easily be extended to cyber systems. (Pfleeger, 2005) Moreover, suppliers' formal arguments can be woven into the system integrator's security and dependability arguments, to show that supply chain issues have been addressed with appropriate levels of care and confidence.
- **Provide economic incentives to encourage "good hygiene"** in individual organizations. Such incentives can speed implementation of protocols (such as DNSSEC), applications and systems that are demonstrably more secure. The incentives should also include rewards for speedy correction of security problems and punishments for lax attention to such problems. There are both public and private precedents for such incentives, such as tax incentives and insurance discounts. Previous attempts at self-regulation have been distinctly unsuccessful; for instance, Edelman (2006) shows that less reputable companies are more likely to buy trust certificates than reputable ones.
- **Encourage research in key multi-disciplinary areas that often get short shrift.** Many security failures occur not because a problem has no solution but because the solution has not been applied. From failure to apply patches promptly to reluctance to thoroughly scrub a system for vulnerabilities, many system problems result from system designers' failure to acknowledge the user's perspective and proclivities. Behavioral science (including psychology and organizational behavior) and behavioral economics have significant potential to improve the security and dependability of the nation's cyber infrastructure. For example, we in the I3P are managing three such projects. The first, on leveraging behavioral science to improve cyber security, is performing a series of carefully-controlled experiments in actual business settings to determine the best ways to improve security awareness and incentivize "good security hygiene." The second, on privacy, is investigating how organizational and national culture influence privacy perception and related behaviors. The third seeks ways to incorporate the user's perspective in the specification, design and testing of cyber security products and services. In the short term, this type of research can improve adoption rates for security technology, thereby reducing the "attack surface" at which malicious attackers take aim.

In the longer term, this research can lead to a more resilient cyber infrastructure that users are eager to use correctly and safely.

References

Anderson, Ross and Tyler Moore, "The Economics of Information Security," *Science* (314:5799), October 2006, pp. 610-613.

Anderson, Ross and Tyler Moore, "Information Security Economics and Beyond," *Proceedings of the Information Security Summit 2008*, available at http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf

Cook, Ian P. and Shari Lawrence Pfleeger, "Security Decision Support Challenges in Data Collection and Use," *IEEE Security & Privacy* 8(3), May 2010, pp. 28-35.

Danezis, George and Ross Anderson, "The Economics of Resisting Censorship," *IEEE Security & Privacy*, 3(1), January 2005, pp. 45-50.

Edelman, Benjamin, "Adverse Selection in Online 'Trust' Certifications," *Fifth Workshop on the Economics of Information Security*, 2006, available at http://www.benedelman.org/publications/advsel-trust.pdf

Geer, Daniel, Charles P. Pfleeger, Bruce Schneier, John S. Quarterman, Perry Metzger, Rebecca Bace and Peter Gutmann, *CyberInsecurity: The Cost of Monopoly*, Computer & Communications Industry Association Report, September 24, 2003, available at https://www.schneier.com/essay-318.html

Knight, John C. and Nancy G. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multi-version Programming," *IEEE Transactions on Software Engineering*, SE-12(1), January 1986, pp. 96-109.

Kunreuther, Howard and Geoffrey Heal, "Interdependent Security," *Journal of Risk and Uncertainty*, 26(2-3), March-May 2003, pp. 231-249.

Pfleeger, Shari Lawrence, "Soup or Art? The Role of Evidential Force in Empirical Software Engineering" *IEEE Software*, January/February 2005.

Pfleeger, Shari Lawrence, "Anatomy of an Intrusion," *IT Professional* 12(4), July 2010, pp. 20-28.

Rantala, Ramona R., *Cybercrime Against Businesses, 2005*, Bureau of Justice Statistics Special Report NCJ 221943, September 2008, available at http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

Rowe, Brent and Michael Gallaher, "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," Workshop on the Economics of Information Security, 2006, available at http://weis2006.econinfosec.org/docs/18.pdf

Rue, Rachel and Shari Lawrence Pfleeger, "Making the Best Use of Cybersecurity Economic Models," *IEEE Security & Privacy* 7(4), July 2009, pp. 52-60.

Sasse, M. Angela, "Usability and Trust in Information Systems," Cyber Trust and Crime Prevention Project, 2004, available at http://hornbeam.cs.ucl.ac.uk/hcs/publications/Sasse_Usability%20and%20trust%20in%20information%20systems_Cyber%20Trust%20&%20Crime%20Prevention%20Project2004.pdf

van Eeten, Michel J.G. and Johannes M. Bauer, *Economics of Malware: Security Decisions, Incentives and Externalities*, STI Working Paper JT03246705, OECD, 29 May 2008.

SHARI LAWRENCE PFLEEGER
4519 Davenport St. NW
Washington, DC 20016-4415
(202) 244-3740
email: shari@pfleeger.com (personal) or shari.l.pfleeger@dartmouth.edu (business)

EDUCATION:
Ph.D., Information Technology and Engineering, George Mason University, 1989
M.S. in planning, The Pennsylvania State University, 1975
M.A. in mathematics, The Pennsylvania State University, 1971
B.A. in mathematics with high honors, Harpur College, Binghamton, New York, 1970
Additional graduate courses: computer science and mathematics, The Pennsylvania State University, 1971-1976; biostatistics, Georgetown University, Washington, DC, 1977-1978
Honorary Doctor of Humane Letters, Binghamton University, May 2000

EMPLOYMENT:
Institute for Information Infrastructure Protection, September 2010 to present. Director of Research. Techical lead for a consortium of 27 major universities, national laboratories and think tanks that work together to examine important issues in information infrastructure protection. Projects address cyber security, dependability, safety, reliability and other aspects of information infrastructure protection. Sources of funding include both government and private enterprise. Projects are multi-institution and multi-disciplinary, and audiences include policy- and decision-makers as well as technologists and users.

RAND Corporation, March 2002 to August 2010. Senior information scientist. Worked with government and private organizations to analyze how information technology supports their mission. Projects focused on strategic planning, policy analysis and decision-making; economics of cyber security; security and privacy issues; insider threat; software cost estimation; information assurance; critical infrastructure protection; measurement and evaluation. Clients have included National Institute of Standards and Technology, Department of Homeland Security, US Air Force, US Patent and Trademark Office, Freddie Mac, US Department of Justice, Defense Advanced Research Projects Agency, Office of Science and Technology Policy, Defense Director of Information Assurance, Bureau of Justice Statistics, US intelligence agencies, US Army.

Recent projects include:
Leveraging Behavioral Science to Reduce Cyber Risk. Research to examine how to apply behavioral science findings to security technology. Funded by the Department of Homeland Security through the Institute for Information Infrastructure Protection, including participation by researchers at MITRE and Dartmouth.

Usability and Security. In conjunction with researchers from NIST and University College London, we looked broadly at how and why the lack of usability prevents security products and processes from being effective. The goal was to produce an initial set of NIST guidelines for evaluating the usability of security products and processes during their design, construction and evolution.

Cyber Security Metrics. Led two projects, one internally funded and one DoD-funded, to develop ways to measure the security of a computer system or network.

Human Behavior, Awareness and Insider Threat. Led project to investigate how to identify cyber security threats from insiders who have legitimate access to system and networks. Funded by the Department of Homeland Security through the Institute for Information Infrastructure Protection. Led teams from Indiana University, Dartmouth College, Columbia University, Cornell University, Purdue University, MITRE and RAND. Emphasis was on multidisciplinary look not only at how technology can support behavior recognition but also on ethical and legislative issues, risk management, and incentives for appropriate behavior.

Economics of Cyber Security. Led project to determine how best to make decisions about investing in cyber security. Funded by the Departments of Homeland Security and Justice through the Institute for Information Infrastructure Protection. Led teams from RAND, MIT Lincoln Laboratory, Dartmouth Tuck Business School, George Mason Law

School, and University of Virginia in providing multidisciplinary view of how to present a business case for cyber security. Included analyses of existing models and framework to understand when to use which models; analysis of current data sources and their pros/cons; recommendations for behavioral, organizational and cultural factors that models should consider; case study of cyber security investment decisions by businesses in the "Internet supply chain." Products: Paper in *Cutter IT Journal*, papers published in *IEEE Security and Privacy*, *IEEE Software*, *IEEE IT Professional*. Similar issues addressed in follow-on I3P project on **Business Rationale for Cyber Security**.

Collecting the Dots. Internal research project to investigate how we know when information is important enough to report it to someone else. Addressed issues of how to communicate the information without flooding the recipient. Proposed initial architecture for a decision support system to help identify emergent situations. Product: Monograph on problem analysis and solution elements.

State Spam and Privacy Laws: An Overview and Analysis. Led project to analyze the current (at the time) state laws related to spam, as well as state and national laws relating to privacy. Funded by the Office of Science and Technology Policy. Products: Memorandum to OSTP with analysis and recommendation; article in *IEEE Security and Privacy*.

Privacy Implications of the Secure Flight Program. Led project to assist the Transportation Security Administration in assessing the privacy implications of its (at that time) proposed Secure Flight program. Product: Facilitated series of meetings of the Secure Flight Working Group, including background analyses of key issues.

Improving the Small Business Innovation Research (SBIR) Program Performance Across the Department of Defense. Member of team that surveyed SBIR recipients and MDAP organizations to determine best practices for SBIR performance. Product: Briefing about findings and best practices.

Software Cost Estimation and Sizing Methods: Issues and Guidelines. Led team investigating the key sources of estimation inaccuracies for the US Air Force. Focused on software sizing and estimation techniques. Product: Monograph describing set of checklists to assist estimators in improving sizing and effort estimates. Follow-on project addressed cost estimation issues for the US Air Force's space systems-related programs.

University of Calgary, January 2006 to June 2008. Adjunct professor of computer science. Collaboration with faculty studying decision-making on software development and maintenance projects.

Pardee Rand Graduate School, September 2006 to May 2010. Affiliate professor in RAND's graduate school of public policy.

Systems/Software, Inc., January 1993 to February 2002. President. Consulting on software engineering, cost estimation, reuse, technology assessment, process and measurement with various clients, including Fannie Mae, Computer Sciences Corporation, Raytheon, American Management Systems, Nokia, Philips, UK Ministry of Defence, European Commission, US Department of Defense, US Patent and Trademark Office and Oak Ridge National Laboratory. Research and analysis focused on reuse, reliability and other software engineering topics. Specialty was evaluation of technology: effectiveness, productivity, quality, trade-off analysis. Work included assessment of maintenance programs; establishment of measurement programs; technology transfer of software engineering techniques; evaluation of suggested best practices; presentation of courses on measurement, experimental design, software engineering decision-making, and technology assessment. Principal investigator, National Science Foundation grant to investigate retrospective data analysis, 1997 to 1998. Principal investigator, National Science Foundation grant to establish national mentoring program for women and minorities in computer science, 1991-1994. Visiting Research Professor at City University of London, with joint appointment to the Department of Business Computing and the Centre for Software Reliability, January 1993 to September 1995: investigated risk engineering techniques for the ESPRIT-funded GOAL project (Dept. of Business Computing); investigated effect of formal methods on dependability for ESPRIT-funded PDCS project (CSR); for DTI-funded SMARTIE project, investigated effectiveness of standards on quality of process and product (CSR). Reviewer for European Commission's ESPRIT-funded SQUID project, examining software quality issues. Taught several graduate classes in software engineering for Department of Business Computing and Department of Computer Science. As Visiting Research Fellow with Computer Science Department, University of North London (1993 to 1995), worked on DTI-funded DESMET project, to evaluate effectiveness of techniques and tools on software development.

University of Maryland Computer Science Department, January 1998 to June 2000. Part-time research scientist and visiting professor. Experimental software engineering research, investigating requirements techniques, effectiveness of practices to determine best practices. Funding from National Science Foundation, ITT, others. Teaching: Fall 1998 Honors undergraduate course: Computing: Separating Hope from Hype. Fall 1999: team taught (with V. Basili and G. Travassos) CMSC 435: Software Engineering. Fall 1999 and Spring 2000: Graduate course MSWE 607: Software Life Cycle Processes.

Howard University Center for Research in Evaluating Software Technology, August 1996 to January 1998. Founder and Director of Center for Research in Evaluating Software Engineering. Professor of systems and computer science in the School of Engineering, Architecture and Computer Science. Director of graduate programs in Systems and Computer Science. Director of the research seminar for graduate students and faculty. Director of industrial-academic partnership projects to evaluate the effectiveness of software engineering techniques and tools. Instructor of several software engineering courses, including Research Methods, Senior Project I and II. Principal investigator, National Science Foundation grant in experimental software systems, 1997-1998.

MITRE Corporation Software Engineering Center, August 1991 to January 1993. Principal Scientist. Leader of strategic planning and technology development for MITRE's Software Engineering Center. Investigated software process and product measurement issues, including models and frameworks using metrics to help customers make decisions about appropriate processes for a given problem. Established process improvement group, leading investigations on process and measurement issues. Project manager and technical leader for Metrics Advisor project, a hypertext tool to recommend metrics based on organizational and project goals and needs. Process assessment/improvement and metrics support to Navy, FAA, Defense Medical Systems Support Center, NASA, others. Member, SEI-MITRE-IDA team to define core set of Defense Department metrics. General technical leadership on software engineering issues, including peer review of both internal and customer tasks and products.

Contel Technology Center Software Engineering Laboratory, May 1989 to June 1991. Principal Scientist. Founded and managed Software Metrics Program for Contel Corporation, a $3 billion telecommuniations company. Metrics program identified by Software Engineering Institute as one of the eleven best programs in the U.S. Defined framework for metrics to be collected throughout the corporation. Designed project databases, metrics toolkits. Designed and integrated metrics tools and decision support tools for process and metrics decisions. Established historical database for metrics data. Supervised AIRMICS-funded research project on the economics of software reuse (the first externally funded research and development program for the Contel Technology Center). Supervised metrics project team. Established summer intern program. Led team to market lab services to internal and external customers. Worked with U.S. Department of State on security requirements and the Orange Book certification process. Research in cost modeling, metrics for requirements analysis and specification, metrics for evaluation of new tools and techniques, metrics for maintenance, integration of metrics in CASE tools and development environments. Supported Contel business units by assisting them in identifying problems, applying software engineering where appropriate.

Systems/Software, Inc., January 1983 to May 1989. Vice President: January 1983 to January 1988; President: January 1988 to May 1989. Designed and developed $1.6 million office automation system for TVA's Office of Natural Resources and Economic Development; established system administrative staff and procedures; developed complete set of automated evaluation tools to determine benefits of system to 2000 users. System analyst for several research-and-development Wang systems. Evaluated series of Wang-based database management systems. Evaluated Navy office automation and communications network. Coordinated training programs for TVA system analysts, for teachers and parents in local school system. Taught Federally Employed Women's National Training Program on office automation. Consultant to Army, Air Force, Navy, State Department, Tennessee Valley Authority, Oak Ridge National Laboratory on Wang computer systems, computer security, software engineering. Designed plan to evaluate secure operating system, developed database to support evaluation. Trained engineers in use of software engineering principles.

System Development Corporation, September 1980 to December 1982. Technical Advisor to Project Control Division. Evaluated existing cost and schedule procedures; designed project control system based on PMS-IV to integrate cost and schedule reporting. Evaluated Computer Systems group; instituted software engineering measures to improve software development performance. Project leader for development of two interactive systems on HP-1000. Project leader for requirements analysis and selection of new computer system. Liaison with customers. Marketing of new customers. Algorithm development to support variety of company projects. General technical advisor to programmers.

Intercon Systems Corporation, August 1978 to August 1980. Senior Analyst. October 1979 to August 1980: Evaluated system design and proposed test plan for large communications system. Evaluated proposals for system enhancements.

Wrote requirements documents; supervised acceptance tests. August 1978 to September 1979: Designed and wrote applications programs for network of PDP-11/70s, including major overhaul of existing code (MACRO assembler, RSX-11D).

PRC Information Sciences Company, September 1976 to August 1978. Senior Associate, November 1977 to August 1978: Member, Applied Research Group. For National Bureau of Standards, reported on methodologies to determine whether a computer system is performing an authorized application. Included evaluation criteria against which to measure each approach and to enable a comparative evaluation. Was member of team to enumerate considerations and trade-offs in developing an interactive computer system. Task included application of operations research techniques to current technological problems. Designed a system to implement the scheduling algorithm evolving from the task. Evaluated proposed system design for the expansion of the National Military Intelligence Center system, including suggestions for database design. Consultant to Georgetown University Medical Center, analyzing data (using SPSS) from the Physicians' Assistant Program. Associate, September 1976 to November 1977: Participated in development of star network of Data General Eclipse and Honeywell 316R computers, driving modified Hazeltine 2000 and teletype terminals plus specialized electronic equipment. System performed message routing and interfaced with similar networks. Designed and implemented queuing and task entry software, systems programs, and device drivers on Honeywell. Task leader for personnel working on Honeywell; supervised four programmers. Generated equations for printing maps on line printer; generated bearing equations for calculating and displaying lines-of-bearing on a CRT.

HRB-Singer, Inc., September 1975 to August 1976. Engineer, Software Development Division. Wrote tape-to-card conversion routines in IBM assembler for use on IBM 360/40; wrote tape-to tape I/O programs in FORTRAN and assembler on PDP 11/45 under DOS. Developed equations and wrote FORTRAN programs to implement map drawing, map projection and satellite orbital calculation software (PDP 11/45 under RSX-11D). Analyzed and generated project data. Headed documentation effort for GACT multi-terminal system; supervised ten people.

The Pennsylvania State University, January 1972 to August 1976. Mathematics instructor, Continuing Education Division, September 1975 to August 1976: Taught calculus classes. Instructor, Department of Mathematics, January 1972 to June 1975: Taught a variety of undergraduate mathematics courses. September 1974 to June 1975: Performed statistical analyses of data gathered at Stone Valley Recreation Area. Developed estimators of hourly population changes in various sections of the recreation area. Produced a simulation model to support decision making and land use planning.

The Anaconda Company, June 1969 to September 1969. Computer programmer. Wrote payroll update and report programs in COBOL and RPG.

AWARDS:

Contel Technology Center and Contel Federal Systems, Citizenship Award, 1989.

Contel Corporation, Citizenship Award, Runner Up, 1989.

Honorary Doctor of Human Letters, Binghamton University, May 2000.

Tower Society Award, Ohio Wesleyan University, 2002.

Luce Foundation Award, 2008.

Most Influential Paper Award: Paper named one of *IEEE Software*'s most influential papers in 25 years.

PROFESSIONAL ACTIVITIES:

Participant in National Science Foundation-funded summer-long Conference on Combinatorial Theory, Bowdoin College, Brunswick, Maine, June 1971.

Consultant, Personnel Standards Committee, National Recreation and Parks Association, January 1975 to January 1976.

Member, State College Municipal Community Appearance and Design Review Board, January 1976 to September 1976.

Secretary, ACM Mid-Southeast Chapter, November 1982 to October 1984.

Vice Chairperson, Knoxville Area Wang User Group, 1987.

Founder and Chairperson, ACM Committee on the Status of Women and Minorities, July 1990 to August 1993.

Principal Investigator, National Science Foundation grant to establish mentoring program for women and minorities in computing, 1991 to 1994.

Principal Investigator, National Science Foundation grant in Empirical Software Systems, investigating experimentation techniques applied to retrospective studies, 1997 to 1998.

Investigator, AIRMICS grant to develop model of the economics of reuse, with Terry Bollinger, 1989 to 1990.

Reviewer for many book publishers and journals, including John Wiley and Sons, Boyd and Fraser, Chapman and Hall, Prentice-Hall, McGraw Hill, Harcourt-Brace-Jovanovich, International Thomson Press, IEEE Computer Society Press, Addison-Wesley publishers, *IEEE Computer, Information and Software Technology, IEEE Software, IEEE Transactions on Systems, Man and Cybernetics, IEEE Transactions on Software Engineering, Software: Practice and Experience, Software Quality Journal, Journal of Systems and Software, Journal of Information Systems, IEEE Spectrum, ACM Transactions on Software Engineering and Methodology*.

Member, Software Engineering Institute Software Measurement Working Group, June 1989 to January 1991.

Member, IEEE Committee on Communications and Information Policy, including membership on Subcommittee on Information Security and Applications, February 1992 to January 1993.

Member, *IEEE Software* Industrial Advisory Board, April 1991 to December 1992.

Member, *IEEE Software* Editorial Board, January 1993 to 1998; Associate Editor-in-Chief, January 1995 to March 1997; Editor, Quality Time column, January 1995 to December 1998.

Member, *IEEE Spectrum* Editorial Advisory Board, September 1993 to January 1997.

Associate Editor, *IEEE Transactions on Software Engineering*, June 1997 to 2001.

Member of the Editorial Board, Software Quality Institute series with Prentice Hall, January 1998 to 2001.

Senior Member, IEEE, IEEE Computer Society, IEEE Technical Council on Software Engineering (at-large representative, July 1996 to June 1999).

Book Review Editor, *IEEE Security and Privacy*, 2003 to 2007

Associate Editor, *IEEE Security and Privacy*, 2007 to present.

Advisory Board Member, Virginia Tech Computer Science Department, 2002 to 2006.

Executive Committee, Institute for Information Infrastructure Protection: Vice Chair Elect 2004-2006; Vice Chair 2006 to 2008.

Member, Institute of Medicine Committee, investigating the Food and Drug Administration's 510(k) process for evaluating the safety of medical devices, April 2010 to July 2011.

Invited speaker:

Conference on Pure Combinatorics, Mathematisches Forschungsinstitut, Oberwolfach, Germany, 1971.

6th Annual Conference on Modeling and Simulation, University of Pittsburgh, April 1975.

3rd NATO Advanced Study Institute on Information Science, Crete, Greece, July-August 1978.

IFAC/IFORS Conference on Information Systems, AFCET, Toulouse, France, March 1979.

Eleventh ASIS Mid-Year Meeting, Knoxville, Tennessee, June 1982.

ACM Mid-Southeast Chapter Meeting, Gatlinburg, Tennessee, November 1983.

ACM Southeast Regional Meeting, Atlanta, Georgia, April 1984.

Office Systems Research Association Conference, Atlanta, Georgia, February 1985.

Syntopican XIII, Washington, DC, June 1985.

Annual Conference, International Society of Wang Users, Boston, Massachusetts, October 1987.

CASE '89, London, England, July 1989.

ACM Lecturer Series, Mary Washington College, Fredericksburg, Virginia, October 1989 and October 1991.

Annual Oregon Workshop on Software Metrics, Portland, Oregon, March 1990 and March 1991.

Reuse and Reengineering Symposium, Alexandria, Virginia, May 1991.

Software Quality Week, San Francisco, California, May 1990 and May 1991.

Washington Ada Symposium, McLean, Virginia, June 1990.
ACM Professional Development Lecturer, University of Maryland, November 1990.
3rd Software Quality Workshop, Alexandria Bay, New York, August 1991.
ACM Computer Science Conference, Kansas City, March 1992.
Software Technology Conference, Salt Lake City, April 1992.
CASE '92, Montreal, Quebec (workshop leader), July 1992.
4th Software Quality Workshop, Alexandria Bay, New York, August 1992.
Pacific Northwest Quality Conference (tutorial instructor and invited speaker), Portland, Oregon, October 1992.
British Telecom Reuse Working Group, London, England, January 1992.
European COCOMO User Group Meeting, Reading, England, February 1992.
International Workshop on Software Reuse (IWSR93), Lucca, Italy, March 1993.
Congress on the Quality of Software 93, Milan, Italy, March 1993.
CSR 93 Conference on Software Measurement, Amsterdam, Netherlands, September 1993.
Applications of Software Measurement 93, Orlando, Florida, November 1993.
British Computer Society Reuse Workshop, London, England, March 1994.
BNR Design Forum, Harlow, England, June 1994.
Congress on the Quality of Software 94, Rome, Italy, September 1994.
European Software Methods Conference, London, England, October 1994.
Keynote Speaker, Philips International Software Conference, Eindhoven, Netherlands, February 1995.
European Software Measurement Conference, Rolduc, Netherlands, May 1995.
NASA Software Engineering Laboratory Annual Workshop, Greenbelt, Maryland, November 1995.
National Institute of Standards and Technology Speaker Series on High Integrity Systems, January 1996.
Speaking tour at major Australian universities, February 1996.
Keynote Speaker, Third International Symposium on Software Measurement, Berlin, Germany, March 1996.
Keynote Speaker, ESCOM 96, Manchester, UK, May 1996.
Applications of Software Measurement 96, San Diego, California, October 1996.
Keynote Speaker, International Conference on Building Quality Software, Hong Kong, December 1996.
Keynote Speaker, Empirical Assessment of Software Engineering (EASE) Conference, Keele, UK, March 1997.
International Conference on Software Maintenance, Bari, Italy, September 1997.
Workshop Leader, Workshop on Empirical Studies of Software Maintenance, Bari, Italy, October 1997.
Tutorial Speaker, International Conference on Software Engineering, Boston, Massachusetts, May 1997.
Keynote Speaker, Society for Information Management workshop, Fairfax, Virginia, March 1998.
Invited Speaker, Software Quality Institute annual symposium, Austin, Texas, April 1998.
Keynote Speaker and Tutorial Presenter, European Software Measurement Conference, Rome, Italy, May 1998.
Keynote Speaker, USPDI Testing Conference, Tyson's Corner, Virginia, June 1998.
Distinguished Lecturer, University of Texas, Austin, December 1998.
Tutorial Presenter, Applications of Software Measurement 99, San Jose, California, February 1999.
Invited Speaker, Litton Software Engineering Conference, Dana Point, California, February 1999.
Keynote Speaker, Empirical Assessment of Software Engineering (EASE) Conference, Keele, UK, April 1999.
Paul Rook Memorial Lecturer, European Software Measurement Conference, Herstmonceaux Castle, UK, April 1999.
Keynote Speaker, Brazilian Software Quality Conference, Curitiba, Brazil, May 1999.
Invited Speaker, Federal University of Rio de Janeiro, Brazil, May 1999.
Keynote Speaker, STEP99, Pittsburgh, Pennsylvania, August 1999.
Keynote Speaker, Colorado Advanced Software Institute Annual Symposium, Denver, Colorado, October 1999.

Tutorial Presenter, Applications of Software Measurement 2000, San Jose, California, March 2000.

Graduation Speaker, Harpur College, Binghamton, New York, May 2000.

Keynote Speaker, International Conference on Software Testing, Bethesda, Maryland, June 2000.

Keynote Speaker, Brazilian Software Quality Conference, Joao Pessoa, Brazil, October 2000.

Tutorial Presenter, ESCOM 2001, London, England, April 2001.

Tutorial Presenter, SEKE 2001, Buenos Aires, Argentina, June 2001.

Keynote Speaker, SEKE 2001, Buenos Aires, Argentina, June 2001.

Keynote Speaker, Brazilian Software Quality Conference, Rio de Janeiro, Brazil, October 2001.

Tutorial Presenter and Invited Speaker, Applications of Software Measurement 2002, Anaheim, California, February 2002.

Workshop Presenter, Computer Sciences Corporation Technology Week, Portovenere, Italy, March 2002.

Tutorial Presenter, International Conference on Software Metrics, Ottawa, Canada, June 2002.

Keynote Speaker, 7th European Software Quality Conference, Helsinki, Finland, June 2002.

Keynote Speaker, International Conference on Software Metrics, Sydney, Australia, September 2003.

Distinguished Speaker, University of Colorado at Colorado Springs, April 2004.

Keynote Speaker, SEKE 2004, Banff, Alberta, Canada, June 2004.

Invited Speaker, University of Calgary, Canada, December 2004.

Keynote Speaker and Tutorial Presenter, Software Education Conference, Wellington, New Zealand, March 2006.

Keynote Speaker and Tutorial Presenter, Software Education Conference, Sydney, Australia, March 2006.

Invited Speaker, Ottawa Software Process Improvement Network, Ottawa, Canada, April 2006.

Invited Speaker, Fourth International iTrust Conference, Pisa, Italy, May 2006.

Invited Speaker, Brazilian Software Engineering Conference, Rio de Janeiro, September 2006.

Keynote Speaker, Conference of the Consortium for Computing Sciences in Colleges, Fredericksburg, Virginia, October 2006.

Invited Speaker, AFCEA Conference on Information Assurance, Washington, DC, February 2008.

Invited Speaker, I3P Workshop on Process Control Systems, Houston, Texas, March 2008.

Invited Speaker, Heritage Foundation Roundtable on Cyber Security, Washington, DC, June 2008.

Invited Speaker, Economics Security Working Group, US Department of Commerce, Washington, DC, June 2008.

Invited Speaker, Information Overload Research Group Forum, New York City, July 2008.

Invited Speaker, Residential Workshop on Countering Insider Threats, Schloss Dagstuhl, Wadern, Germany, July 2008.

Moderator, Senate Homeland Security Forum on Cyber Security and Human Behavior, Washington, DC, September 2008.

Invited Speaker, Fourth World Software Quality Congress, Bethesda, Maryland, September 2008.

Keynote Speaker, The Malicious Exploitation of Information Systems: Preventing the Rise of the Insider Threat, University College London, November 2008.

Invited Speaker, Workshop on the Economics of Information Security, London, England, June 2009.

Invited Speaker, Suspicious Behavior and Insider Threat Workshop, Lansdowne, Virginia, September 2009.

Keynote Speaker, Workshop Anual do MPS (Annual Brazilian Workshop on Process Improvement), Campinas, Brazil, October 2009.

Invited Speaker, Software Assurance Forum, Arlington, Virginia, November 2009.

Invited Speaker, SEI Workshop on Insider Threat, Arlington, Virginia, June 2010.

Program Chairperson:

ACM Mid-Southeast Chapter Summer Meeting, Gatlinburg, Tennessee, June 1981.

ACM Mid-Southeast Region 25th Anniversary Meeting, Gatlinburg, Tennessee, November 1984.

ACM Mid-Southeast Chapter Autumn Meeting, Gatlinburg, Tennessee, November 1987.

Fourth International Symposium on Software Measurement, Albuquerque, New Mexico, November 1997.

International Conference on Software Maintenance, Amsterdam, September 2003.

General Chairperson:

Second International Symposium on Software Measurement, London, England, October 1994.

Third Workshop on Empirical Studies of Software Maintenance, Bethesda, Maryland, November 1998.

Organizer, First International Workshop on Assurance Cases, DSN04 (Dependable Systems and Networks), Florence, Italy, July 2004.

PUBLICATIONS:

TEXTBOOKS:

Introduction to Discrete Structures, with David W. Straight. John Wiley and Sons, 1985.

Software Engineering: The Production of Quality Software, Macmillan, 1987, 1991 (second edition).

"The Economics of Reuse," with T. Bollinger, chapter in *The Economics of Information Systems and Technology* edited by R. Veryard, Butterworths Publishers, 1990.

"Setting Up a Metrics Program in Industry," chapter in *Software Quality Assurance and Measurement*, edited by N. Fenton and R. Whitty, International Thomson Press, 1995.

"Integrating Process and Measurement," chapter in *Software Measurement: Understanding Software Engineering*, edited by Austin Melton, International Thomson Press, 1995.

Applying Software Metrics, co-edited with Paul Oman, IEEE Computer Society Press, 1997.

Software Metrics: A Rigorous and Practical Approach, with Norman Fenton, second edition, International Thomson Press, 1997.

"Experimentation in Software Engineering," chapter in *Advances in Computers*, Academic Press, 1997.

"Use Realistic, Effective Software Measurement," chapter in *Constructing Superior Software*, edited by Paul C. Clements, Software Quality Institute Series, Macmillan Technical Publishing, New York, 1999.

Solid Software, with Chuck Howell and Les Hatton, Prentice Hall, 2001.

"Using Mentoring to Advance Females and Minorities in a Corporate Environment," with Norma T. Mertz, chapter 15 in *The Organizational and Human Dimensions of Successful Mentoring Programs and Relationships*, edited by Frances Kochan, Information Age Publishing, Greenwich, CT, September 2002.

Security in Computing, fourth edition, with Charles P. Pfleeger, Prentice Hall, 2007

"Making Executive Mentoring Work in IT," with Norma Mertz, *Encyclopedia of Gender and Information Technology*, edited by Eileen Trauth, Information Science Publishing, 2006.

Software Engineering: Theory and Practice, Prentice Hall, 1998, 2001, 2005 (third edition with Joanne Atlee), 2009 (fourth edition with Joanne Atlee).

Applying Computer Security: A Threat/Vulnerability/Countermeasure Approach, with Charles P. Pfleeger, Prentice Hall, to appear 2011.

INVITED AND SPONSORED PAPERS:

"Path-Cycle Ramsey Numbers," with T. D. Parsons, *Notices of the American Mathematical Society*, February 1973.

"Cycle-Star Ramsey Numbers," *Notices of the American Mathematical Society*, June 1973.

"Bipartite Ramsey Numbers,"*Notices of the American Mathematical Society*, October 1973.

"Simulating a Recreational Lake Facility," with G. Kleindorfer, *Proceedings of the Sixth Annual Conference on Modeling and Simulation*, April 1985.

"Simulating a Recreational Lake Facility," with G. Kleindorfer, Center for the Study of Environmental Policy, Paper No. 14, June 1975.

"Computer Safeguards: Application Characteristics," with G. Blomgren and M. Goldstein, National Bureau of Standards Study Paper, June 1978.

"Interactive Use of Computers in Recreational Planning," *Proceedings of the Third NATO Advanced Study Institute on Information Science*, July to August 1978.

"Control of Information: The Political Implications," *Proceedings of the Eleventh ASIS Mid-Year Meeting*, June 1982.

"Modeling Office Automation Benefits," *Proceedings of the OSRA Conference*, February 1985.

"An Object-Oriented Approach to Knowledge Acquisition," George Mason University Technical Report, 1988.

"A History of Software Cost Models," George Mason University Technical Report, 1989.

"The Economics of Software Reuse," with T. Bollinger, Contel Technology Center Technical Report CTC-TR-089-014, December 1989.

"Recommendations for an Initial Set of Software Metrics," Contel Technology Center Technical Report CTC-TR-89-017, December 1989.

"Software Metrics Tools Evaluation," with Joseph Fitzgerald, Jr., Contel Technology Center Technical Note CTC-TN-090-017, September 1990.

"Software Estimation for Object-Oriented Systems," with J. D. Palmer, *Proceedings of the International Function Point Users Group*, November 1990.

Guest Editor, *IEEE Software* special issue on Measurement-based Process Improvement, with H.D. Rombach, July 1994.

Series on Experimental Design and Analysis in Software Engineering, *ACM SIGSOFT Software Engineering Notes*, October 1994 through December 1995.

"Software Engineering: Viewpoint," *IEEE Spectrum*, January 1995.

"Reuse Measurement and Evaluation," *American Programmer*, November 1995.

Guest Editor, *IEEE Software* special issue on Software Quality on Trial, with B. A. Kitchenham, January 1996.

"Software Quality: the Elusive Target," with B. A. Kitchenham, *IEEE Software*, January 1996.

Guest Editor, *IEEE Software* special issue on Measurement, March 1997.

"Using Measurement to Support Software Testing," *Dr. Dobb's Journal*, February 1998.

"Speeding Technology Transfer," *Managing System Development*, Spring 1999.

"Making Software Development Investment Decisions," with John Favaro, *ACM SIGSOFT Software Engineering Notes*, September 1998.

"Decisions and Delphi: The Dynamics of Group Estimation," with Martin Shepperd and Roseanne Tesoriero, *Proceedings of the Brazilian Software Engineering Conference*, Joao Pessoa, Brazil, October 2000.

"Principles of Survey Research," series in six parts, with Barbara A. Kitchenham, *ACM SIGSOFT Software Engineering Notes*, November 2001 and forward.

"Solid Software: Is It Rocket Science?" *Proceedings of the 7th European Conference on Software Quality*, Springer, 2002.

"A Gift of Impact," book review of *A Gift of Fire*, by Sara Baase, second edition, in *IEEE Security and Privacy*, 2004.

"Everything You Wanted to Know About Privacy (But Were Afraid to Ask)," book review of *Privacy: What Developers and IT Professionals Should Know*, by J. C. Cannon, *IEEE Security and Privacy*, May-June 2006.

"Why We Won't Review Books By Hackers," with Charles Pfleeger, *IEEE Security and Privacy*, July-August 2006.

Guest Editor, *IEEE Security and Privacy* special issue on managing security, with Roland Trope and Charles Palmer, May 2007.

"Insiders Behaving Badly," with Joel Predd , Jeffrey Hunker, and Carla Bulford, *IEEE Security and Privacy*, July-August 2008, pp. 66-70.

"Software Metrics: Progress After 25 Years?" *IEEE Software*, November-December 2008, pp. 32-34.

Guest Editor, *IEEE Security and Privacy* special issue on insider threats, with Salvatore Stolfo, November/December 2009.

"Addressing Insider Threats," with Salvatore Stolfo, *IEEE Security and Privacy*, November/December 2009, pp. 10-13.

Guest Editor, *IEEE Security and Privacy* special issue on usability and security, with Mary Frances Theofanos, to appear in March 2011.

Guest Editor, *IEEE Software* special issue on software business, with John Favaro, to appear in May 2011.

REFEREED PAPERS:

"Path-Cycle Ramsey Numbers," with R. Faudree, T. Parsons and R. Schelp, *Discrete Mathematics*, vol. 10, 1974.

"Project Control Through Integration of Cost and Schedule," *Proceedings of APMS-82*, August 1982.

"A Model of Office Automation Benefits," with J. N. Cline, *Journal of the Office Systems Research Association*, Spring 1985.

"Measuring Improved Productivity," *Journal of the Office Systems Research Association*, Spring 1988.

"A Transaction Flow Approach to Software Security Certification for Document Handling Systems," with C. P. Pfleeger, *Computers and Security*, October 1988.

"The Incorporation of Metrics in CASE Tools," *Proceedings of CASE '89*, July 1989.

"Penetration Testing Methodology," with C. P. Pfleeger and M. F. Theofanos, *Computers and Security*, vol.8, November 1989.

"The Economics of Reuse: Issues and Alternatives," with T. Bollinger, *Proceedings of the Annual National Conference on Ada Technology*, March 1990.

"Software Metrics in the Process Maturity Framework," with C. McGowan, *Journal of Systems and Software*, July 1990.

"A Software Metrics Toolkit: Support for Selection, Collection and Analysis" with J. Fitzgerald, *Proceedings of the Eighth Annual Pacific Northwest Software Quality Conference*, October 1990.

"The Economics of Reuse: Issues and Alternatives," with T. Bollinger, *Information and Software Technology*, December 1990.

"A Framework for Software Maintenance Metrics," with S. Bohner, *Proceedings of the Conference on Software Maintenance*, December 1990.

"Process Maturity as a Framework for CASE Tool Selection," *Proceedings of CASE '90*, December 1990.

"A Software Metrics Database: Support for Analysis and Decision-Making," with J. Fitzgerald, *Proceedings of the Annual National Conference on Ada Technology*, March 1991.

"Software Metrics Reporting: Presentation of Multiple Metrics for Analysis of Improvement," with J. Fitzgerald and D. Rippy, *Proceedings of the Third Annual Oregon Workshop on Software Metrics*, March 1991.

"A Model of Software Effort and Productivity," *Information and Software Technology*, April 1991.

"A Software Metrics Toolkit: Support for Selection, Collection and Analysis," with J. Fitzgerald, *Information and Software Technology*, September 1991.

"A Framework for Security Requirements," *Computers and Security*, October 1991.

"Process Maturity and CASE Tool Selection," *Information and Software Technology*, November 1991.

"Using Multiple Metrics for Analysis of Improvement," with J. Fitzgerald and D. Rippy, *Software Quality Journal*, March 1992.

"Measuring Software Reliability," *IEEE Spectrum*, August 1992.

"Lessons Learned in Building a Corporate Metrics Program," *IEEE Software*, May 1993.

"Science and Substance: A Challenge to Software Engineers," with N. Fenton and R. Glass, *IEEE Software*, July 1994.

"The Economics of Reuse: New Approaches to Modelling Cost," with T. Bollinger, *Information and Software Technology*, August 1994.

"Evaluating Software Engineering Standards," with N. Fenton and S. Page, *IEEE Computer*, September 1994.

"Executive Mentoring: What Makes It Work?," with N. Mertz, *Communications of the ACM*, January 1995.

"Case Studies for Method and Tool Evaluation," with B. Kitchenham and L. Pickard, *IEEE Software,* July 1995.

"Experimental Design and Analysis," *Annals of Software Engineering*, November 1995.

"Developing a Metrics Plan," *Journal of Systems and Software*, November 1995.

"How Do Formal Methods Affect Code Quality?," *Proceedings of the NASA/SEL Workshop*, November 1995.

"Towards a Framework for Software Measurement Validation," with B. Kitchenham and N. Fenton, *IEEE Transactions on Software Engineering*, December 1995.

"Measuring Reuse: A Cautionary Tale," *IEEE Software*, July 1996.

"Wavefront: A Goal-driven Requirements Process Model," with Mary Theofanos, *Information and Software Technology*, August 1996.

"Investigating the Influence of Formal Methods," with Les Hatton, *IEEE Computer*, February 1997.

"Status Report on Software Measurement," with Bill Curtis, Ross Jeffery and Barbara Kitchenham, *IEEE Software*, March 1997.

"Understanding and Improving Technology Transfer in Software Engineering," *Journal of Systems and Software*, July 1999.

"Albert Einstein and Empirical Software Engineering," *IEEE Computer*, October 1999.

"Technology Transfer: Marketing Technology to Software Practitioners," with Winifred Menezes, *IEEE Software*, January/February 2000.

"Risky Business: What We Have Yet to Learn About Software Risk Management," *Journal of Systems and Software*, 53(3), September 2000.

"Preliminary Guidelines for Empirical Research in Software Engineering," with Barbara Kitchenham, Lesley Pickard, Peter W. Jones, David Hoaglin, Khaled El Emam and Jarrett Rosenberg, *IEEE Transactions on Software Engineering*, August 2002.

"What Can Software Engineering Learn From Soccer?," *IEEE Software*, November 2002.

"A Case Study of Maintenance Estimation Accuracy," with Barbara Kitchenham, Beth McColl and Sue Eagan, *Journal of Systems and Software*, vol. 64, November 2002.

"Canning Spam: Proposed Solutions to Unwanted E-Mail," with Gabrielle Bloom, *IEEE Security and Privacy*, March/April 2005.

"Soup or Art? The Role of Evidential Force in Empirical Software Engineering," *IEEE Software*, January/February 2005.

"Investing in Cyber Security: The Path to Good Practice," with Rachel Rue, Jay Horwitz and Aruna Balakrishnan, *Cutter IT Journal*, 19(1), January 2006.

"I'll Buy That! Cyber Security in the Internet Marketplace," with Martin Libicki and Michael Webber, *IEEE Security and Privacy*, May/June 2007.

"A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making," with David Ortiz and Rachel Rue, Workshop on the Economics of Information Security, June 2007.

"Investing in Cyber Security: Clearing the Path to Good Practice," with Rachel Rue, *IEEE Software*, January/February 2008.

"Choosing a Security Option: The InfoSecure Methodology," with Thomas Ciszek, *IEEE IT Professional*, September/October 2008, pp. 46-52.

"Software Metrics: Progress After 25 Years?," *IEEE Software*, November/December 2008, pp. 32-34.

"Making the Best Use of Cyber Security Economic Models," with Rachel Rue, *IEEE Security and Privacy*, July/August 2009, pp. 52-60.

"Useful Cyber Security Metrics," *IEEE IT Professional*, 11(3), May/June 2009, pp. 38-45.

"Security Through Information Risk Management," with M. Eric Johnson and Eric Goetz, *IEEE Security and Privacy*, May/June 2009, pp. 45-52.

"Harmonizing Privacy with Security Principles and Practices," with Charles Pfleeger, *IBM Journal of Research and Development*, 53(2), 2009.

"Insiders Behaving Badly: Addressing Bad Actors and Their Actions," with Joel Predd, Jeffrey Hunker and Carla Bulford, *IEEE Transactions on Information Forensics and Security* 5(1), March 2010.

"Why Security Measurement is Hard," with Robert K. Cunningham, *IEEE Security and Privacy*, July/August 2010, pp. 46-54.

"Anatomy of an Intrusion," *IEEE IT Professional*, special issue on cyber security, July/August 2010, pp. 20-28.

"Security Decision Support: Challenges in Data Collection and Use," with Ian Cook, *IEEE Security and Privacy*, May/June 2010, pp. 28-35.

"Addressing Information Risk in Turbulent Times," with M. Eric Johnson, to appear in *IEEE Security and Privacy*.

RAND PUBLICATIONS:
Report number: RAND/PM-1579-OSTP
Year: 2003
Title: State Spam and Privacy Laws: An Overview and Analysis
Authors: Shari Lawrence Pfleeger and Gabrielle Bloom.

Report number: RAND/CF-187-OSTP
Year: 2003
Title: Technology Transfer of Federally Funded R&D: Perspectives from a Forum.
Author(s): Mark Wang, Shari Lawrence Pfleeger, David M. Adamson, Gabrielle Bloom, William P. Butz, Donna Fossum, Mihal Gross, Charles Kelley, Terrence K. Kelly, Aaron Kofner, Helga Rippen

Report number: RAND/OP-103-RC
Year: 2004
Title: Collecting the Dots: Problem Formulation and Solution Elements.
Authors: Martin C. Libicki, Shari Lawrence Pfleeger

Report number: RAND/PM-1690-A
Year: 2004
Title: High Performance Computing Opportunities and Challenges for Army R&D. No.1, Interim Report.
Authors: Robert H. Anderson, Anthony C. Hearn, Rosalind Lewis, John Matsumura, Shari Lawrence Pfleeger, Isaac Porsche, Randall Steeb, Felicia Wu

Report number: RAND/MG-269-AF
Year: 2005
Title: Software Cost Estimation and Sizing Methods: Issues and Guidelines
Authors: Shari Lawrence Pfleeger, Felicia Wu and Rosalind Lewis

Report number: RAND/DB-490-OSD
Year: 2006
Title: Evaluation and Recommendations for Improvement of the Department of Defense Small Business Innovation Research (SBIR) Program.
Authors: Bruce J. Held, Thomas Edison, Shari Lawrence Pfleeger, Philip S. Antón, John Clancy

Report number: RAND/OP-140-RC
Year: 2006
Title: Revisiting US-VISIT: US Immigration Processes, Concerns and Consequences
Authors: David-Santana Ortiz, Shari Lawrence Pfleeger, Aruna Balakrishnan and Merril Miceli

Report number: RAND TR-303
Year: 2006
Title: The Global Technology Revolution: 2020
Authors: Richard Silberglitt, Philip Anton, David Howell, Anny Wong, Susan Bohandy, Natalie Gassman, Brian Jackson, Eric Landree, Shari Lawrence Pfleeger, Elaine Newton and Felicia Wu

Report number: RAND DRR-4088-1-AF
Year: 2007
Title: Improving the Cost Estimating Process for U.S. Air Force Space Systems: An Assessment of Organization, Personnel and Processes
Authors: Obaid Younossi, Kevin Brancato, Cynthia R. Cook, Bernard Fox, John C. Graser, Mark A. Lorell, Shari Lawrence Pfleeger, Jerry M. Sollinger

Report number: RAND MG-690
Year: 2008

Title: Improving the Cost Estimation of Space Systems: Past Lessons and Future Recommendations.
Authors: Obaid Younossi, Kevin Brancato, Cynthia R. Cook, Bernard Fox, John C. Graser, Mark A. Lorell, Shari Lawrence Pfleeger, Jerry M. Sollinger

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 112th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Shari Lawrence Pfleeger

Capacity in which appearing: (check one)

● Individual

○ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented:

FISCAL YEAR 2011

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
2006-CS-001-000001 to I3P	Dept. of Homeland Security – NCSD	$200,000 to support Shari out of $22 3M total	Cyber Security Collaboration and Information Sharing
70NANB10H214 to I3P	Dept. of Commerce-NIST	$80,000 for Shari of $175,000 total	Assessing and Enhancing the Action-Awareness Framework

FISCAL YEAR 2010

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contract to RAND	OSD	$49,552,804 total	FFRDC Research
Contract to RAND	Air Force	$45,467,025 total	FFRDC Research
Contract to RAND	Army	$28,096,000 total	FFRDC Research
Contract to RAND	Dept. of Commerce-NIST	$209,818 total	Develop Action-Awareness Framework
Contract to RAND from I3P	DHS	$89,026	Planning grant for Human Behavior and Cyber Security
Contract to RAND from I3P	DHS	$47,917	Human Behavior and Cyber Security Project

FISCAL YEAR 2009

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contract to RAND	OSD	$49,734,998 total	FFRDC Research
Contract to RAND	Air Force	$44,591,840 total	FFRDC Research
Contract to RAND	Army	$31,680,000 total	FFRDC Research

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2011):______________________________;
Fiscal year 2010:____________________________________;
Fiscal year 2009:____________________________________.

Federal agencies with which federal contracts are held:

Current fiscal year (2011):______________________________;
Fiscal year 2010:____________________________________;
Fiscal year 2009:____________________________________.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2011):______________________________;
Fiscal year 2010:____________________________________;
Fiscal year 2009:____________________________________.

Aggregate dollar value of federal contracts held:

Current fiscal year (2011):______________________________;
Fiscal year 2010:____________________________________;
Fiscal year 2009:____________________________________.

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2011):______________________________;
Fiscal year 2010:______________________________;
Fiscal year 2009:______________________________.

Federal agencies with which federal grants are held:

Current fiscal year (2011):______________________________;
Fiscal year 2010:______________________________;
Fiscal year 2009:______________________________.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2011):______________________________;
Fiscal year 2010:______________________________;
Fiscal year 2009:______________________________,

Aggregate dollar value of federal grants held:

Current fiscal year (2011):______________________________;
Fiscal year 2010:______________________________;
Fiscal year 2009:______________________________.

Remarks of Gerry Cauley, President and Chief Executive Officer North American Electric Reliability Corporation

House Armed Services Committee Subcommittee on Emerging Threats and Capabilities February 11, 2011

Good morning Chairman Thornberry, Ranking Member Langevin, Members of the Subcommittee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have over 30 years experience in the bulk power system industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program.

Background

NERC's mission is to ensure the reliability of the bulk power systems of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system (BPS).[1] In 2007, NERC was designated the Electric Reliability Organization (ERO) by FERC in accordance with the Energy Policy Act of 2005 and our reliability standards became mandatory across the BPS. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 002 through 009 which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards are the only mandatory cybersecurity standards in place across the critical infrastructure sectors of North America. Subject to FERC oversight, NERC enforces these standards, which are developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's evolutionary dependency on electricity, the electric grid is one of the nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by man. It provides electricity to over 334 million people, is capable of generating over 830 gigawatts of power over 211,000 miles of high voltage transmission lines and represents over $1 trillion in assets. The electricity being used in this room right now is being generated and transmitted in real time over a complex series of lines and stations from possibly as far away as Ontario or Tennessee. As complex as it is, few machines are as robust as the BPS. Decades of experience with hurricanes, ice storms, and other natural disasters as well mechanical breakdowns, vandalism and sabotage, have taught the electric industry how to build strong and reliable networks. The knowledge that disturbances

[1] The Bulk Power System (BPS) is defined as generation and transmission of electricity greater than 100kv, in contrast to the distribution of electricity to homes and businesses at lower voltages.

on the grid can impact operations thousands of miles away has influenced the electric industry culture of planning, operating and protecting the BPS.

The Cybersecurity Challenge for the Grid

Along with the rest of our economy, over the past few decades the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the reliability of the BPS. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the BPS requires constant vigilance and expertise. An increasing amount of resources and skill are required to mitigate vulnerabilities and maintain the integrity and availability of the BPS.

The assets that make up the BPS are varied and widespread. Consequently, the architecture within the systems varies from operator to operator. However, the computer systems that monitor and control BPS assets are based on relatively few elements of technology. Due to increasing efficiencies and globalization of vendors, the universe of suppliers for industrial control systems is limited. This trend is leading toward a fairly homogenous technological underpinning and, as older proprietary technology is replaced, the variation may decrease further.

For example, the bulk power system could be as vulnerable to digital threats as IT systems, but with far more critical implications, as the recent Stuxnet virus has shown. As proprietary industrial control systems continue to integrate Commercial Off-The-Shelf (COTS) systems, these platforms could inherit the embedded vulnerabilities of those systems. As illustrated by Stuxnet, industrial control system software can be changed and data can be stolen without intrusions even being detected. These injection vectors serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code that could result in changes to set points and switches as well as the alteration or suppression of measurements.

Establishment and continued refinement of enterprise risk-based programs, policies and processes to prepare for, react to, and recover from cybersecurity vulnerabilities need to continue to be a high priority for the industry. The bulk power system has not yet experienced wide-spread debilitating cyber-attacks; the most significant contributing factor is the traditional physical separation between the industrial control system environment and the business and administrative networks. The increased sharing of internet and computer networking by control systems and business and administrative networks simply means that digital infrastructures that were formerly physically separated are now becoming susceptible to common threats that were previously unknown in control system environments.

The Role of NERC and Critical Infrastructure Protection Reliability Standards

The NERC CIP reliability standards create a useful baseline of security, but they should not be interpreted (or expected) to render an entity invulnerable. Rather, the NERC CIP standards require electric sector entities to develop a risk based security policy based upon their own specific assets, architecture and exposure. This policy, if properly implemented, will provide insight into the entity's systems and provide the opportunity to mitigate potential threats and vulnerabilities before they are exploited. While the electric sector is the only critical infrastructure sector to have mandatory cybersecurity standards, simple compliance with the NERC CIP standards is only an initial element in properly securing the BPS. There is no single security asset, security technique, security procedure or security standard that even if strictly followed or complied with will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best practices call for additional processes, procedures and technologies beyond those required by the CIP standards. Simple implementation of enforceable standards, while valuable and a necessary first step, should not be seen as the security end-state. It's important here to emphasize the difficulty of addressing grid security through a traditional regulatory model that relies principally on mandatory standards, regulations, and directives. The defensive security barriers mandated by CIP standards can be effective in frustrating ordinary hackers or would be copper thieves by increasing the costs and resources necessary to harm to the grid. They will not, however, stop the determined efforts of the intelligent, adaptable adversaries supported by nation states or more sophisticated terrorist organizations. NERC is moving forward with a number of actions to complement our mandatory CIP Standards and provide enhanced resilience for the grid. As chair of the Electricity Sub- Sector Coordinating Council (ESCC), I work with industry CEO's and our partners within the government to discuss and identify critical infrastructure protection concepts, processes and resources as well as facilitate information sharing about cyber vulnerabilities and threats. This type of public/private partnership is key to coordination and communication efforts on cybersecurity topics and initiatives. NERC is also developing a North American cyber security exercise to prepare for and test a national response plan for the electric sector.

The most effective approach for combating advanced adversaries is to apply resiliency principles, as outlined in a set of nine recommendations the National Infrastructure Advisory Council delivered to the White House in October 2010. I served on that Council along with a number of nuclear and electric industry CEO's. Resiliency requires a more proactive readiness for whatever may come our way. Resiliency includes providing an underlying robust system; the ability to respond in real-time to minimize consequences; the ability to restore essential services; and the ability to adapt and learn. The industry is already resilient in many aspects, based on system redundancy and the ability to respond to emergencies. To further enhance resiliency, examples of the NIAC team's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved information sharing by government regarding actionable threats and vulnerabilities; 3) cost recovery for security investments driven by national policy or interests; and 4) a national strategy on spare equipment with long lead times, such as transformers. At NERC, we are working with stakeholders to develop programs that build upon the resiliency inherent in the grid to better secure critical assets and ensure the continued reliability of the BPS.

Information Exchange is Critical

It is important to note that NERC and the electric industry can only develop risk based security policies that deal with the risks they are aware of. It is impractical, inefficient and impossible to defend against all possible risks, threats or vulnerabilities. Entities must prioritize their resources to ensure that they are protected against those risks that pose the greatest harm to their assets, business and clients. The electric industry is in the best position to understand the impact that a particular event or incident could have on the BPS, but they do not have the same access to actionable intelligence and analysis that the Government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and unknown vulnerabilities. Too often we have heard from Government agencies that the threats are real, but are given little or no additional information. This leads to frustration among the private sector leaders who are unable to take fact-based responsive measures due to ill-defined and nebulous threat information.

Improving the amount and quality of actionable intelligence is a priority for NERC and it manifests itself in a number of projects in which we are engaged with the Departments of Defense and Homeland Security. NERC is currently working with both DoD and DHS to finalize a memoranda of understanding regarding sharing of bi-directional actionable intelligence. Under this agreement, NERC, as the Electric Sector Information Sharing and Analysis Center (ES-ISAC), will act as a clearing house, disseminating actionable intelligence including classified contextual information to appropriately cleared staff within the BPS community. NERC will also provide anonymous situational awareness back to DoD and DHS analysts to supplement the information received from the intelligence community. We see this effort as crucial to improving the level of threat awareness within the industry.

NERC-DOD Collaboration

Few elements of our society are able to generate enough of their own electricity so as to be independent of the electric grid and this includes the Department of Defense. The vast majority of our nation's military facilities purchase their electricity from private sector power companies, creating a symbiotic relationship that has endured for over 100 years. Defense Department leadership recognizes that the BPS is vital to the readiness and overall effectiveness of the Department's mission and has reached out to NERC to collaborate on ensuring the continued reliable supply of electricity to our defense facilities.

To that end, I recently traveled to Colorado Springs to meet with officials from U.S. NORTHCOM where we discussed collaborating on various electric grid focused activities including participation in the 2011 SecureGrid Exercise, providing electric sector situational awareness and collaborating on the Joint Capability Technology Demonstration (JCTD) Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). The latter project is being proposed to discover how specific facilities could develop small reliable "micro-grids" on a short-term or emergency basis. Similarly, NERC is discussing a project with U.S. NORTHCOM to develop case studies at critical military installations to further understand the requirements for "flow of power" and the implications to military readiness.

NERC is engaged with other agencies and DOE National Laboratories to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the BPS. We are working with Pacific Northwest National Laboratory (PNNL) on developing certification guidelines for Smart Grid Cyber Operators and discussing the creation of a technical method to verify compliance with Aurora vulnerability mitigation. Similarly we are working with the Idaho National Laboratory (INL) to promote Cyber Security Evaluation Tools (CSET) for use within the electric sector and partnering with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to share threat, vulnerability and security incident information. We are also exploring collaboration with INL to expand benchmarking of vendor products and systems that improve cybersecurity protection, especially within the BPS.

Additionally as announced last week, NERC is actively engaged with the Department of Energy and the National Institute of Standards and Technology (NIST) in developing comprehensive cybersecurity risk management process guidelines for the entire electric grid, including the BPS and distribution systems. We believe this to be particularly important with the increasing availability of "smart grid" technologies. While the majority of technology associated with the "smart grid" is found within the distribution system, without appropriate safeguards and security processes and procedures in place, vulnerabilities realized within the distribution system could potentially impact the BPS. It is incumbent upon everyone engaged in the smart grid implementation that appropriate security applications and technologies be built into the system to prevent additional threats and vulnerabilities.

The title of this hearing today is "What should be the Department of Defense's role in cybersecurity?" Clearly, the Department of Defense has important resources, invaluable expertise and critical mission needs when put in context of the Advanced Persistent Threat (APT). At the same time, defining the Department's role on this issue is not easy when so many critical assets are privately owned. Increases in information sharing and growing trusted relationships between government agencies and private sector organizations can go a long way in improving the overall security posture of our critical infrastructure. Leadership is key. Without the institutional courage to be first and the humility to receive constructive criticism we will never advance the security conversation beyond just that of an exchange of positions. We must develop operational strategies that are capable of adjusting and growing to match the evolving threat.

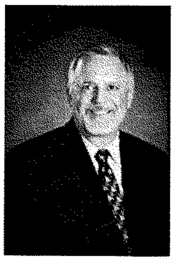
Conclusion

As our nation moves forward and continues to become more dependent upon electricity and information systems, it is imperative that we come to grips with how we secure those systems that enable our way of life. Government must provide leadership and appropriate support in addressing the question of how to integrate security into society. Industry must be willing to use its expertise and resources to further the goals of our nation to make it stronger as well as more prosperous. The cybersecurity challenges facing us are not intractable - they are the result of our own great innovation and can be overcome through our own great ingenuity.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Gerry W. Cauley



Gerry W. Cauley is President and Chief Executive Officer of the North American Electric Reliability Corporation (NERC), effective January 1, 2010. Mr. Cauley has served since 2007 as President and Chief Executive Officer of the SERC Reliability Corporation, a nonprofit corporation responsible for promoting and assessing the reliability and critical infrastructure protection of the bulk power system in 16 southeastern and central states. Previously, Mr. Cauley worked at NERC for ten years in positions of increasing responsibility, ultimately as Vice President and Director of Standards. He was instrumental in preparing NERC's application to become the Electric Reliability Organization and spearheaded NERC's development of an initial set of standards to ensure the reliability of the bulk power system in North America. Mr. Cauley was also a lead investigator of the August 2003 Northeast blackout and coordinated all aspects of the NERC Y2k Program, supervising the reporting and readiness of 3,100 electric organizations in the United States and Canada.

Prior to joining NERC in 1996, Mr. Cauley served for six years as the program manager of grid operations and planning at the Electric Power Research Institute. He was also a training consultant for ten years in the areas of electric system operations, nuclear and fossil plant operations, substations, and distribution. He served five years as an officer in the U.S. Army Corps of Engineers.

Mr. Cauley holds a B.S. degree from the U.S. Military Academy at West Point, an M.S. degree from the University of Maryland in Nuclear Engineering, and an MBA from Loyola College - Baltimore. Mr. Cauley is a registered Professional Engineer in the Commonwealth of Virginia.

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 112th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Gerry W. Cauley, President & CEO, NERC

Capacity in which appearing: (check one)

○ Individual

● Representative

If appearing in a representative capacity, name of the company, association or other entity being represented:

FISCAL YEAR 2011

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
NO			

FISCAL YEAR 2010

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
NO			

FISCAL YEAR 2009

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
NO			

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Federal agencies with which federal contracts are held:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Aggregate dollar value of federal contracts held:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Federal agencies with which federal grants are held:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Aggregate dollar value of federal grants held:

Current fiscal year (2011): NO ;
Fiscal year 2010: NO ;
Fiscal year 2009: NO .

Statement of Gregory T. Nojeim

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

Before the House Committee on Armed Services,
Subcommittee on Emerging Threats and Capabilities

On

The Role of the Department of Defense in Cybersecurity

February 11, 2011

Chairman Thornberry, Ranking Member Langevin, and Members of the Subcommittee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittee for examining the role of the Department of Defense in cybersecurity. Today, I will briefly outline the cybersecurity threat and discuss how to avoid cybersecurity measures that would infringe on privacy or innovation or unintentionally undermine security itself. I will emphasize that private network operators, not the government, should monitor and secure private sector systems, while the Department of Defense secures military systems and the Department of Homeland Security secures civilian government systems. To the extent that DOD entities have information and expertise that would help private sector operators and DHS with their cybersecurity activities, mechanisms must be developed to permit DOD to share that information and expertise. I also will discuss some incremental changes in the law that may enhance information sharing without eroding privacy. Finally, I will discuss the role that identity and authentication measures, if properly designed and deployed, can play in enhancing security while also protecting privacy.

The Cybersecurity Threat

It is clear that the United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. In

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

2009, the *Wall Street Journal* reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.[2] Last year, Google revealed that it had been subjected to a major espionage attack originating in China aimed at stealing personal information about human rights activists and Google's own proprietary information.[3] DOD agencies, which have developed capabilities to launch cyber attacks on adversaries' information systems, have sounded alarms about what a determined adversary could do to critical information systems in the U.S. Both offensive and defensive aspects of the issue may have been illustrated by the Stuxnet worm, which, allegedly designed with the involvement of the U.S. government, penetrated the control systems of centrifuges Iran was using to refine uranium, causing hundreds of the centrifuges to spin out of control and damage themselves.[4]

It is also clear that the government's response to this threat has been inadequate. The Department of Homeland Security has been repeatedly criticized[5] for failing to

[2] Gorman, Siobhan, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal,* http://online.wsj.com/article/SB124027491029837401.html, April 21, 2009.

[3] Nakashima, Ellen, Google To Enlist NSA To Help It Ward Off Cyberattacks, *The Washington Post,* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html, February 4, 2010. Information from over 30 other technology, defense, energy and financial firms was also compromised in related attacks.

[4] Broad, William, et al., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times,* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1, January 15, 2011.

[5] *See, e.g.,* Government Accountability Office, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* http://www.gao.gov/new.items/d061087t.pdf, Testimony of GAO's David A. Powner, Director, Information Technology Management Issues, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, September 13, 2006. In 2008, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability,* http://www.gao.gov/products/GAO-08-588, July 2008. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities: *Cybersecurity, Continued Federal Efforts Are Needed to Protected Critical Systems and Information.* Testimony of GAO's Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, June 25, 2009. In 2010, GAO found continued shortcomings. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed,* GAO-11-24, October 6, 2010, http://www.gao.gov/products/GAO-11-24.

develop plans for securing key resources and critical infrastructure, as required in the Homeland Security Act of 2002.[6] President Obama's national security and homeland security advisors completed a cyberspace policy blueprint on April 17, 2009, but implementation of those measures was slowed by the Administration's failure timely to appoint the cybersecurity official in the White House who could drive policy development and coordinate implementation of a government-wide plan.

In the meantime, the Department of Defense has stood up its own cybercommand to oversee the military's efforts to protect its own 15,000 computer networks.[7] Commanded by General Keith Alexander - who also heads the NSA - it is housed at Fort Meade alongside the NSA. It became operational on May 21, 2010, pulling together information operations expertise from components of the Army, Navy and Air Force and launching a program to recruit a cadre of cyberwarriors. In this environment - a plodding DHS and a slowed-down White House, an emergent Cybercommand with expertise, a complex threat environment with many actors and networks that interconnect and that all need to be defended - it is tempting to ask Cybercommand and the NSA to do it all.

We urge you to resist that temptation and instead send a clear message in support of the statement Deputy Secretary of Defense William Lynn, III made last November:

> [Cybercommand] is not intended to be the militarization of cyberspace. It will be responsible for DOD's networks - the dot-mil world. Responsibility for civilian networks - dot-gov - stays with the Department of Homeland Security, and that's exactly how it should be.[8]

In support of this effective allocation of responsibilities, this Subcommittee should encourage DOD entities to share cybersecurity information that would be useful for private sector entities and to support, with limitations, the work of the DHS in defending the civilian government domain. It should also watch out for "mission

[6] P.L. 107-296, Section 201(d)(5).

[7] The United States Cybercommand is subordinate to the U.S. Strategic Command and is headquartered in Fort Meade, Maryland where NSA is also headquartered. Its mission statement, from the U.S. Strategic Command Fact Sheet:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

http://www.stratcom.mil/factsheets/Cyber_Command/.

[8] Lynn, William J. III, Deputy Secretary of Defense, speech delivered November 12, 2009 at the Defense Information Technology Acquisition Summit in Washington, D.C. http://www.defense.gov/speeches/speech.aspx?speechid=1399.

creep" that would find Cybercommand and the NSA conducting activities not in support of others that go beyond defense of .mil networks.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. It is absolutely essential to draw appropriate distinctions between military government systems, civilian government systems, and systems owned and operated by the private sector. Policy towards government systems, both those in the military domain and those under .gov, can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

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

While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the Internet into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls a critical element of the electric power grid or of a user of an information system containing classified information, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

In sum, CDT believes that cybersecurity legislation and policy should not treat all critical infrastructure information systems the same. Instead, a sectoral approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet critical to new economic models, human development, and civic engagement are not regulated in ways that could stifle innovation, chill free speech or violate privacy.

Network Providers – Not the Government – Should Monitor Privately-Owned Networks for Intrusions

When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama said:

> *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

CDT strongly agrees. No governmental entity – including any element of DOD and DHS – should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. Most critical infrastructure computer networks are maintained by the private sector. Private sector operators already monitor those systems on a routine basis to detect and respond to attacks as necessary to protect their networks, and it is in their business interest to continue to ramp up these defenses. Indeed, providing reliable networks is essential to maintaining their business.

Transparency and the Role of the NSA and Cybercommand in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency and the Cybercommand should lead or play a central role in the government-wide cybersecurity program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government and that Cybercommand will be better resourced than DHS to do this work. However, expertise in spying does not necessarily entail superior expertise in all aspects of cybersecurity. The answer to insufficient resources at DHS should be augmentation of those resources, not abdication of its mission. Moreover, there is serious concern that if a DOD entity were to take the lead role in cybersecurity for civilian unclassified systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, thereby increasing the likelihood of failure and decreasing the effectiveness of the effort even in terms of security.

Over 85% of critical infrastructure information systems are owned and operated by the private sector, which also provides much of the hardware and software on which government systems rely, including the government's classified systems. The private sector has valuable information about vulnerabilities, exploits, patches and responses. Private sector operators may hesitate to share this information if they do not know how it will be used and whether it will be shared with competitors. Private sector cooperation with government cybersecurity effort depends on trust. A lack of transparency undermines trust and has hampered cybersecurity efforts to date.

For many reasons, openness is an essential aspect of any national cybersecurity strategy. Without transparency, there is no assurance that cybersecurity measures adequately protect privacy and civil liberties and adhere to Fair Information Practice and due process principles. Transparency is also essential if the public is to hold the government accountable for the effectiveness of its cybersecurity measures and for any abuses that occur.

NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. For these reasons, among others, NSA should not be given a leading role in monitoring the traffic on unclassified civilian government systems, nor in making decisions about cybersecurity as it affects such systems; and its role in monitoring private sector systems should be even smaller. Instead, procedures should be developed for ensuring that whatever expertise and technology NSA has in discerning attacks is made available to a civilian agency.

Likewise, Cybercommand, which will also operate largely in secret, should focus on securing the .mil domain. Mission creep into the .gov domain and the private sector should be guarded against. The lead for cybersecurity operations should stay with the Department of Homeland Security. Maintaining this division of labor will benefit both security and liberty. It will require governmental entities and the private sector to share cybersecurity information, and will require DOD entities to share human resources and expertise with DHS.

-- Sharing human resources and expertise: the DOD/DHS Cybersecurity MOU

On September 27, 2010, DHS and DOD signed a Memorandum of Understanding setting forth the terms by which they would provide personnel, equipment and facilities to increase inter-departmental collaboration and support and synchronize each other's cybersecurity operations.[9] Under the agreement, DHS sends teams to the NSA to plan and synchronize cyber-defense, learn about acquisition detection technologies and coordinate on civil liberties protections. NSA sends a team of cryptologists and operations professionals to the DHS network operations center to support DHS operations. NSA experts would work alongside DHS cybersecurity teams to help bring those teams up to speed quickly.

As CDT said when the MOU was made public in October, this kind of arrangement, if of limited duration, might represent the best way to leverage the NSA's defensive expertise domestically without the negatives associated with it being secretive, operating without public oversight, and, when operating abroad, bending and breaking local rules.[10] CDT has long advocated building up the civilian cybersecurity capability by leveraging the expertise of the NSA precisely to reduce the need of DHS to rely directly on NSA. Once DHS has built the necessary expertise, the existing MOU can expire. This Subcommittee could play an important role in overseeing this arrangement to make sure that it is benefitting both security and liberty.

[9] Memorandum Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity, effective September 27, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[10] Leslie Harris, President and CEO of the Center for Democracy & Technology in the Huffington Post, October 15, 2010, http://www.huffingtonpost.com/leslie-harris/dhs-nsa-in-cybersecurity_b_764289.html.

-- Sharing information: Disclosures from the private sector to the government

Current law gives providers of communications services substantial authority to monitor their own systems and to disclose to military and civilian governmental entities, and to their peers, information about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider. 18 U.S.C. 2511(2)(a)(i). This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications (18 U.S.C. 2702(b)(3)) and customer records (18 U.S.C. 2702(c)(5)) to any governmental or private entity.[11] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[12] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass. 18 U.S.C. §2511(2)(i).

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity, including DOD. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. The extent of service provider disclosures to DOD entities for self-defense purposes is not known publicly. We urge the Subcommittee to consider imposing a requirement that the extent of such information sharing be publicly reported, in de-identified form, both to assess the extent to which beneficial information sharing is occurring, and to guard against ongoing or routine disclosure of Internet traffic to DOD entities under the self-defense exception.

There is a widespread perception that cybersecurity information sharing as practiced is inadequate and there is some concern that the provisions of the Wiretap Act and ECPA are impediments to information sharing. This issue must be

[11] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. 2702(b)(8) and (c)(4).

[12] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. 2510(21).

approached very cautiously, for exceptions intended to promote information sharing could end up severely harming privacy.

First, it should be noted that there has not been sufficient analysis to determine what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[13] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs)[14] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[15] The suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[16] Industry is

[13] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

[14] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established Information Sharing and Analysis Centers (ISACs) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See*, THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION 1 (Jan. 2009), *available at* http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

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

[16] *See* DHS Press Release announcing opening of the NCCIC, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

now represented at the NCCIC[17] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, industry self-interest, rather than government mandate, should be relied on to facilitate information sharing from the private sector to governmental entities. Congress should explore whether additional market-based incentives could be adopted to encourage the private sector to share threat and incident information and solutions. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information about threats and attacks in cyberspace by terrorists and others.

CDT strongly disagrees with proposals to solve the information-sharing dilemma by simply expanding government power to obtain privately held data. We urge the Congress to steer clear of proposals to give a governmental entity wide-ranging authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities.[18] Such an approach would be dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. Collecting large quantities of sensitive information into a common database can also undermine security because such a database could, itself, become a target for hackers.

While, as noted above, current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, we have heard concern that the provisions do not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. Many types of attacks could affect multiple providers, and disclosure by one entity about such an attack could be helpful to others. Therefore, there might be a need for a very narrow exception to the Wiretap Act and ECPA that would permit disclosures about specific attacks and malicious code on a voluntary basis, and that would immunize companies against liability for these disclosures. The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited.

[17] *See* DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full time IT-ISAC analyst at the NCCIC, November 18, 2010, http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.

[18] For an example of such a proposal, see Section 14 of the Cybersecurity Act of 2009 as introduced in the 111th Congress, S. 773.

Overall, given the risks to privacy, we urge the Congress to take only incremental approaches to information sharing, avoiding more radical approaches, such as permitting or mandating broad sharing of information that may be personally identifiable. In addition, because the existing privacy protections in ECPA have been outpaced by the development of technology, we also urge that any changes to ECPA to facilitate cybersecurity information sharing are counterbalanced with enhanced privacy protections.

-- Sharing information: Disclosures from the government to the private sector

DOD and DHS have legitimate roles, to the extent they have special expertise, in helping the private sector develop effective monitoring systems to be operated by the private sector. Most of the federal government's cybersecurity effort regarding private sector networks should focus on improving information sharing and otherwise strengthening the ability of the private sector to protect private sector networks. This is particularly true for DOD entities such as NSA, which have identified attack signatures that private sector entities may not be aware of. Ways should be found for the NSA to share such information with private sector network operators to help them identify attacks at an early stage, defend in real time against attacks, and secure their networks against future attack. Ideally this sharing would happen through DHS and would help DHS develop its own corresponding capacity.

Much has been said about the problem of sharing classified information with private sector owners and operators of critical information systems. This Subcommittee could make a substantial contribution to cybersecurity by taking steps to ensure that attack signatures are not unnecessarily classified and by working to ensure that providers have personnel who are cleared to receive the attack signatures that must remain classified.

The Government Should Monitor Its Own Networks for Intrusions, But Privacy Concerns Need to Be Addressed

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has the responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that exercise of the First Amendment rights of free speech and to petition the government will be chilled if communications between Americans their government are routinely accessed and shared with law enforcement and intelligence agencies. While the Fourth Amendment may not come into play because those communicating with governmental entities necessarily reveal their communications - including content - to the government, the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government.

Another important consideration is the question of how likely it is that private-to-private information may be accessed inadvertently through systems intended to detect intrusions against government computers. While we do not quarrel with the notion that DOD should monitor its own systems for intrusions, the role of intelligence and law enforcement agencies such as the NSA and the FBI in the intrusion detection enterprise with respect to civilian government networks must be carefully considered. Generally, Fair Information Practice principles should be applied to minimize the amount of personally identifiable information collected by the government, to limit its use of this information, and to notify users of this information collection and disposition.[19]

Under current law, all federal departments and agencies must adhere to information security best practices. Generally, these practices include the use of intrusion detection systems.[20] In an effort to improve security, the government has developed and is deploying the Einstein intrusion detection and prevention system. According to a May 19, 2008 Privacy Impact Assessment[21] and a January 9, 2009 opinion of the DOJ Office of Legal Counsel,[22] Einstein 2 is being deployed at participating federal agency Internet Access Points. Einstein 2 assesses network traffic against a pre-defined database of signatures of malicious code and alerts U.S. CERT to malicious computer code in network traffic. While the signatures are not supposed to include personally identifiable information ("PII") as defined by DHS, they do include Internet Protocol addresses, and the alerts that Einstein 2 generates for U.S. CERT may include PII.[23] In addition to using attack signatures, Einstein 2

[19] The Department of Homeland Security's Chief Privacy Officer issued a memorandum in late 2008 to describe how DHS would apply FIPS. *Privacy Policy Guidance Memorandum,* issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[20] Einstein 2 PIA, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf (May 19, 2008), p. 2.

[21] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

[22] Stephen. G. Bradbury, Principal Deputy Assistant Attorney General, *Legal Issues Relating To the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,* January 9, 2009, http://www.justice.gov/olc/2009/e2-issues.pdf. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes, and an August 14, 2009 opinion from the Obama Justice Department's Office of Legal Counsel affirms that conclusion. http://www.justice.gov/olc/2009/legality-of-e2.pdf.

[23] The PIA for Einstein 2 makes it clear that, for example, Einstein 2 will collect an email address when the source of malicious code it detects is attached to an email address. Moreover any "flow record" (a specialized summary of a suspicious communication) that Einstein routinely generates will generally include IP address and time stamp, which are widely regarded as personally identifiable.

also detects anomalous network traffic on a particular system and alerts U.S. CERT to those anomalies.

A successor, Einstein 3, is being tested with an undisclosed ISP and an undisclosed federal agency. It will have the added capability of intercepting threatening Internet traffic before it reaches a government system. According to the Privacy Impact Assessment DHS issued in connection with these tests,[24] Einstein 3 will use intrusion detection technology developed by the NSA and will adapt threat signatures developed by NSA in the course of its foreign intelligence work and by the DOD in connection with its information assurance mission. It will also use commercially available threat signatures. A key feature of Einstein 3 is that it operates on the network of an ISP providing service to the government instead of on the network of the federal agency that is being protected. One critically important question is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications passing over the ISP's network.

According to the Einstein 3 PIA, the participating federal agency will provide Internet Protocol addresses to the ISP, which will use them to distinguish traffic to or from that agency from other traffic. This is a logical, but by no means fool proof method of identifying the targeted traffic. IP addresses can be re-allocated and become outdated. If Einstein were to analyze private-to-private communications, it would likely be conducting an unlawful interception under the electronic surveillance laws. The Intelligence Authorization Act for FY 2010 requires reports to Congress about the privacy impact of Einstein and any other similar cybersecurity programs as well as information about the legal authorities for the programs and about any audits that have been conducted or are planned for the programs.[25] The Subcommittee should consider whether it would be appropriate for it to conduct oversight to determine the extent to which Einstein information flows back to DOD entities and the uses to which this information is being put.

Other questions about the Einstein intrusion detection system include:

- What personally-identifiable information has Einstein collected so far?
- What have law enforcement and intelligence agencies done with Einstein information that is shared with them, and more to the point, to what extent is the system being used to identify people who should be prosecuted or people who are of intelligence interest, even if that is not its primary purpose?
- To what extent are private sector operators keeping information about communications that appear to match attack signatures?
- How should users be notified that their visits to government websites and

[24] Privacy Impact Assessment for the Initiative Three Exercise, March 18, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf.

[25] Section 336 of the Intelligence Authorization Act for FY 2010, Pub. L. No. 111-259.

> their email communications with government employees are being scanned for security reasons? [26]

The lack of transparency around Einstein highlights a broader concern about the federal government's cybersecurity program: excessive secrecy undermines public trust and communications carrier participation, both of which are essential to the success of the effort. The government needs to publicly disclose sufficient details about Einstein and other programs to be able to assure both the public at large and private sector communications service providers that the confidentially of personal and proprietary communications will be respected.

"Active Defense" and the First Amendment

Some DOD cybersecurity activities are expected to go beyond the kind of monitoring envisioned in the Einstein program. We also urge you to tread carefully in the area of "active defense" in the cybersecurity arena because of the First Amendment concerns raised by some active defense activities. Most cybersecurity measures today involve taking defensive steps, such as using firewalls and protecting sensitive information through authentication and authorization systems.

DOD officials and other experts speak of "active defense" and of offensive measures that would involve reaching out beyond the boundaries of military networks that must be protected and into other networks to hunt for malicious software.[27] For example, General Keith Alexander, head of Cybercommand and of the NSA, reportedly seeks authority to shut down parts of adversaries' computer networks to pre-empt a cyberattack against U.S. targets.[28] The risk here is that attacking computers in one country can unintentionally disrupt communications in another and disrupt the ability of people in the U.S. to legitimately access information that may be housed abroad. Moreover, because attribution is difficult in cyberspace, there is heightened risk that a defensive attack aimed at the source of malware will target another victim of the attack, instead of the attacker itself.

For all of these reasons, we urge you to take great care when considering these measures, and that this Subcommittee exercise its oversight authority over such measures keeping in mind the First Amendment rights of Americans.

[26] For a fuller listing of open questions about the Einstein Intrusion Detection System, see Center for Democracy & Technology, *Einstein Intrusion Detection System: Questions That Should Be Addressed*, http://www.cdt.org/security/20090728_einstein_rpt.pdf.

[27] The line between "active defense" and "offensive" cyber operations is a blurry one, and we do not attempt here to delineate what activities fall into each category.

[28] Nakashima, Ellen, Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield, *The Washington Post*, November 6, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html?wprss=rss_world.

Presidential Authority in Cybersecurity Emergencies

Some have proposed that the President or the Department of Homeland Security ought to be given authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[29] When the government of Egypt cut off Internet services on January 27, 2011 to much of its population in order to stifle dissent in an uprising, it magnified concerns about extending cybersecurity emergency authority to the U.S. President. It illustrated the First Amendment concerns that would attend use of such authority in the U.S. The authority to shut down or limit communications traffic should extend only to governmental systems (presumably, the government already has the authority to disconnect its own systems from the Internet), but should not extend to those maintained by private sector entities.

To our knowledge, no circumstance has yet arisen that could justify a governmental order to limit or cut off Internet traffic to a particular privately-owned and controlled critical infrastructure system when the operators of that system think it should not be limited or cut off. They already have control over their systems and strong financial incentives to quarantine network elements that need such measures. They already limit or cut off Internet traffic to particular systems when they need to do so. They know better than do government officials whether their system needs to be shut down or isolated.

The list of potential unintended consequences to both the economy and to critical infrastructures themselves from a shut down of Internet traffic is long. It could interfere with the flow of billions of dollars necessary for the daily functioning of the economy. It could deprive doctors of access to medical records. Users of those systems, which may include government personnel, state and local emergency first responders and civilian volunteers, could find themselves with crippled communications capability in a crisis. It could deprive manufacturers of critical supply chain information. It could have world wide effect because much of the world's Internet traffic goes through the United States.

Even if such power over private networks were exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system.

Finally, giving the government the power to shut down or limit Internet traffic would also create perverse incentives. Private sector operators will be reluctant to share information if they know the government could use that information to order them to shut them down. Conversely, when private operators do determine that

[29] In the 111th Congress, Section 18 of the Cybersecurity Act of 2009, S. 773 and Section 201 of the Protecting Cyberspace as a National Asset Act, S. 3480 both included such provisions.

shutting down a system would be advisable, they might hesitate to do so without a government order and could lose precious time waiting to be ordered by the government to shut down so that they would less likely be held liable for the damage a shut down could cause others.

We urge you to reject proposals to give the President or another governmental entity power to limit or shut down Internet traffic to privately held critical infrastructure systems.

Building Privacy into Identity and Authentication Requirements Designed to Thwart or Discourage Malicious Activity

One of the most talked-about approaches to preventing and tracing cyber attacks by terrorists and others is to improve identity and authentication of those who would seek access to the system that must be protected. If an attack cannot be attributed to a particular person because the person cannot be identified, it is difficult to prosecute the perpetrator or deter the attack. However, while identification and authentication will likely play a significant role in securing critical infrastructure, identity and authentication requirements should be applied judiciously to specific high value targets and high-risk activities.

Some have argued for broad authentication mandates across the Internet – including calls for "Internet passports." Mandating strong identity and authentication measures for routine Internet interactions could seriously compromise user privacy, slow on-line interactions and transactions so much that their utility would be impaired, and fundamentally limit the ways in which people use the Internet.

While identity and authentication measures are important elements of cybersecurity, they can either promote privacy or threaten it, depending on how they are designed and implemented. For example, the fact that some transactions or interactions are anonymous may *enhance* the privacy and security of those transactions. Moreover, the right to speak anonymously enjoys constitutional protection.[30] On the other hand, authentication can also enhance privacy. For example, authenticating a party to a transaction may advance a privacy interest by preventing identity fraud. Depending on how the authentication system is designed, disclosing personally identifiable information to facilitate authentication may put privacy at risk or it may increase privacy. For example, it is possible to disclose data to establish trusted credentials that can be used for many on-line transactions, thereby eliminating the need to provide such information for each transaction and to many different entities.[31] Instead of submitting personal information to 10

[30] *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334 (1995).

[31] Center for Strategic and International Security, *Report of the CSIS Commission on Cybersecurity for the 44th Presidency,*

websites in order to make 10 purchases, the information could be submitted once to a credentialing organization that would perform the authentication necessary to the other transactions. At least for systems used by the private sector, government officials are not well equipped to resolve the complex design and implementation issues that must be addressed to ensure that such a system enhances privacy and security rather than undermining them. Accordingly, policymakers should be hesitant to impose identity mandates on the private sector.

Identity and authentication requirements should adhere to the principles of proportionality and diversity.[32] Under the proportionality principle, if a transaction has high significance and sensitivity and an authentication failure carries with it significant risk, it may be more appropriate to require authentication and the collection of more sensitive information to authenticate. Conversely, certain transactions do not need high degrees of authentication, or any at all. This principle applies in both the private and public sectors, but private sector operators - who know their systems best - are in the best position to decide what level of identity and authentication should be required for their own systems and transactions, depending on the degree of risk posed and the degree of trust that is called for. Private sector operators, such as those in the financial sector, already use various security measures related to online services such as banking and e-commerce. In addition, in light of the federal government's poor historical track record on securing its own systems, it may not be the best entity to put in charge of credentialing or other centralized online security activities.

Under the diversity principle for privacy in identity management schemes, it is better to have multiple identification solutions, because use of a single identifier or credential creates a single target for privacy and security abuses. A single identifier also allows for multiple transactions and interactions to be tied to that identifier, permitting potentially invasive data surveillance. Instead, identification and enrollment options should function like keys on a key ring, with different identities

http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, December, 2008, p. 63. The CSIS report advocates strong authentication of identity for the information and communications technology sector, and the energy, finance and government services sectors. It also recognizes that authentication requirements should be proportional to the risk they pose and that consumers should have choices about the authentication they use.

[32] CDT has outlined these and other Privacy Principles for Identity in the Digital Age. Version 1.4 of the principles, released in December 2007, can be found here: http://www.cdt.org/security/identity/20080108idprinciples.pdf. The privacy principles for identity that extend beyond proportionality and diversity are based on Fair Information Practice principles, and include specifying the purpose for the system being used, limiting the use and the retention period of personal information collected, giving individuals control and choice over identifiers needed to enroll in a system to the extent this is possible, providing notice about collection and use of personally identifiable information, security against misuse of the information provided, accountability, access and data quality.

for different purposes.[33] One model that holds great promise is the "user-centric" identity model, in which the user logs into a Web site through a third party identity provider, who passes on information at the user's request to the Web site in order to authenticate the user.

The White House Cyberspace Policy Review embraced the diversity and proportionality principles by calling for an array of interoperable identity management systems that would be used only for what it called "high value" activities, like certain smart grid functions, and then only on an opt-in basis. It also called for the federal government to build a security-based identity management vision and strategy for the nation, in collaboration with industry and civil liberties groups.

Likewise, the draft National Strategy for Trusted Identities in Cyberspace (NSTIC) envisions an identity eco-system led by various private sector identity providers. It is not a "government ID for the Internet." If such an ID were created, it would not be trusted and would be little used. Instead, NSTIC properly relies on private sector entities to create identities that operate across many platforms. It also accounts for the need to have a range of levels of assurance for interaction on the Internet, ranging from completely anonymous to highly assured.

We urge the Congress to reject sweeping identity mandates and instead support identity initiatives that are led by the private sector and based on the federated model, as recommended in the NSTIC.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. Effective policies will preserve the open, decentralized, user-controlled, and innovative nature of the Internet and will tailor solutions to the systems that need protection.

Private network operators should monitor their own networks for evidence of intrusion and malicious code. Current law provides adequate authority for such monitoring, but may need to be clarified while ensuring that "self protection" measures do not become backdoors for governmental monitoring of private networks.

The DOD should focus on securing the .mil domain and should provide information and human resources to help DHS to monitor and secure the .gov domain. Intrusion detection and prevention activities should be designed and implemented so as not

[33] *See,* Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age,* http://www.cdt.org/security/identity/20080108idprinciples.pdf, December 2007.

to chill the right to free speech and the right to petition the government. Intrusion detection/prevention programs such as Einstein should be made more transparent.

Privacy and security are not a zero sum game. Measures intended to increase the security of communications and transactions – such as identity and authentication requirements – need not threaten privacy and indeed may enhance it if properly deployed.

GREGORY T. NOJEIM

Contact Information:

Center for Democracy & Technology
1634 Eye St. NW, Suite 1100
Washington, DC 20006
(202) 407-8833

Personal Information:

Date of Birth:	1959
Citizenship:	USA
Gender:	Male

Employment History:

2007- present: Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
Washington, DC

Activities and Duties:
Direct a CDT project that focuses on national security, the Fourth Amendment, and civil liberties. Developed expertise in legal aspects of electronic surveillance and in protecting privacy as against intrusion by the government. Spearheaded CDT's efforts to promote judicial supervision of Americans' private telephone and email conversations in connection with legislation to update the Foreign Intelligence Surveillance Act. Deeply involved in a multiyear project to update the Electronic Communications Privacy Act to account for advances in technology. Leader of CDT's cybersecurity work, testifying in both the House and Senate about the impact of cybersecurity proposals on privacy, civil liberties and innovation.

Publication: Cybersecurity and Freedom on the Internet, 4 *Journal of National Security Law and Policy,* 2010.

1995-2007: Associate Director & Chief Legislative Counsel; Legislative Counsel
ACLU Washington Legislative Office
Washington, DC

Activities and Duties:
As Legislative Counsel: Advocated on privacy, electronic surveillance, national security and immigration matters. Testified in Congress, prepared briefings for Hill staff, drafted constitutional analyses of pending legislation and did extensive public speaking. Advised White House Comm'n on Aviation Safety and Security on civil liberties issues.
As Associate Director & Chief Legislative Counsel: Had overall responsibility for the activities of ACLU's legislative and policy counsels. Reviewed legal and

constitutional analyses of pending legislation and developed legislative strategies. Served as an institutional spokesperson.
Appointed Co-Chair, Coordinating Committee on National Security and Civil Liberties of the American Bar Association's Section on Individual Rights and Responsibilities, and was one of the lead drafters of the ABA's policy on the state secrets privilege.

1991-1995: Director of Legal Services
American-Arab Anti-Discrimination Committee
Washington, DC

Activities and Duties: Directed and implemented ADC's legal functions, litigation, and policy analysis, focusing on civil rights, human rights and immigration matters.

1985-1988: Associate
Kirkpatrick & Lockhart
Washington, DC

Activities and Duties: Drafted legal memoranda and documents incidental to corporate transactions in connection with mergers and acquisitions, immigration, international trade, and small business start-ups.

Education:

1985: Juris Doctor, University of Virginia School of Law, Charlottesville, VA
1981: BA Political Science, University of Rochester, Rochester, NY
1977: Graduated as class valedictorian from Churchville-Chili Sr. High School in Churchville, NY.

DISCLOSURE FORM FOR WITNESSES
CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 112th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee.

Witness name: Gregory Nojeim, Center for Democracy & Technology

Capacity in which appearing: (check one)

○ Individual

● Representative

If appearing in a representative capacity, name of the company, association or other entity being represented:

FISCAL YEAR 2011

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant

FISCAL YEAR 2010

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Harvard Pilgrim	Food & Drug	$7,584	Sentinel Privacy Panel:
Healthcare Institute	Administration		Detection & Analysis of
(a subgrant)			Adverse Events related to
			Regulated Products in
			Automated Healthcare
			Data

FISCAL YEAR 2009

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant

Federal Contract Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2011):________________________;
Fiscal year 2010:____________________________;
Fiscal year 2009:____________________________.

Federal agencies with which federal contracts are held:

Current fiscal year (2011):________________________;
Fiscal year 2010:____________________________;
Fiscal year 2009:____________________________.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2011):________________________;
Fiscal year 2010:____________________________;
Fiscal year 2009:____________________________.

Aggregate dollar value of federal contracts held:

Current fiscal year (2011):________________________;
Fiscal year 2010:____________________________;
Fiscal year 2009:____________________________.

Federal Grant Information: If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2011):__________;

Fiscal year 2010: One__________;

Fiscal year 2009:__________.

Federal agencies with which federal grants are held:

Current fiscal year (2011):__________;

Fiscal year 2010: Subgrant: Food and Drug Administration__________;

Fiscal year 2009:__________.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2011):__________;

Fiscal year 2010: Sentinel Privacy Panel__________;

Fiscal year 2009:__________.

Aggregate dollar value of federal grants held:

Current fiscal year (2011):__________;

Fiscal year 2010: $7,584__________;

Fiscal year 2009:__________.