S. Hrg. 111–724

CYBER SECURITY—2009

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

APRIL 28, 2009

CYBER SECURITY: DEVELOPING A NATIONAL STRATEGY

SEPTEMBER 14, 2009

CYBER SECURITY: PROTECTING INDUSTRY AGAINST GROWING THREATS

Available via http://www.gpoaccess.gov/congress/index.html

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

U.S. GOVERNMENT PRINTING OFFICE
51–019 PDF WASHINGTON : 2010

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.

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE McCASKILL, Missouri
JON TESTER, Montana
ROLAND W. BURRIS, Illinois
MICHAEL F. BENNET, Colorado

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
JOHN McCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina
ROBERT F. BENNETT, Utah

Michael L. Alexander, *Staff Director*
Deborah P. Parkinson, *Professional Staff Member*
Adam R. Sedgewick, *Professional Staff Member*
Brandon L. Milhorn, *Minority Staff Director and Chief Counsel*
Asha A. Mathew, *Minority Senior Counsel*
John K. Grant, *Minority Counsel*
Trina Driessnack Tyrer, *Chief Clerk*
Patricia R. Hogan, *Publications Clerk and GPO Detailee*
Laura W. Kilbride, *Hearing Clerk*

CONTENTS

WITNESSES

Thursday, April 28, 2009

Monday, September 14, 2009

Alphabetical List of Witnesses

Page

APPENDIX

RESPONSES TO POST-HEARING QUESTIONS FOR THE RECORD

ADDITIONAL INFORMATION FOR THE RECORD

CYBER SECURITY: DEVELOPING A NATIONAL STRATEGY

THURSDAY, APRIL 28, 2009

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

The Committee met, pursuant to notice, at 10:05 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, Landrieu, Burris, and Collins.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Thanks to the witnesses and others who are here.

The topic of this hearing is our national strategy for cyber security. I am going to put my statement in the record and just speak for a few moments.[1]

It is a series of facts that brings the Committee here and why we are grateful to a very distinguished and informed group of witnesses for helping us.

The first fact is that America cyberspace is constantly under attack. The second is, the best that I can determine, our defenses to those attacks are inadequate. The third fact is that the Obama Administration, building on work done by the Bush Administration, has just completed a 60-day review of our cyber policy and structures, and we expect soon to see release of that report.

The fourth fact is that the Department of Homeland Security (DHS), which was created out of this Committee and over which we maintain oversight and monitoring our responsibility, has the unique authorities given to it under the statute with regard to cyber security.

The fifth fact, may be a probability, I believe, as part of the reaction to the report that Melissa Hathaway is doing for President Obama, that we will be asked to consider, and should consider, some legislative changes or authorizations regarding the role of the Homeland Security Department in its responsibility to protect critical parts of America's cyberspace, particularly, the non-defense, governmental cyberspace and to be the main point of coordination with the private sector.

[1] The prepared statement of Senator Lieberman appears in the Appendix on page 71.

So this hearing is really an opportunity for us to learn from the four of you at this quite significant, potentially transformational moment in the history of America's relationship to cyber warfare, really. I want to just briefly develop a few of those realities.

First, it is very clear, if I can use a harsh word, but I will use it because it is relevant, our enemies in cyberspace, whether they are individual hackers, foreign governments, business competitors, organized crime groups, or terrorists, seem too often to be one step ahead of our efforts to deter them, and that gap must be closed.

From 2003's SQL Slammer to the most recent Conficker worm, thousands of worms, viruses, and so-called malware have infected and disabled computers around the world and put sensitive data at risk of loss, theft, or improper disclosure. Privacy breaches are a regular occurrence with identity thefts, stolen credit cards, or exposure of financial information. Within the Federal Government, millions of dollars worth of equipment has been lost and the personal information of millions of veterans, as one example, compromised.

In a speech last week, Melissa Hathaway, who is the Acting Senior Director for Cyberspace for both the National and Homeland Security Councils, told of an incident in which 130 automatic teller machines (ATMs), in 49 cities around the world, were illicitly emptied by cyber theft over a single 30-minute period. I mean, that is a stunning reality.

The *Wall Street Journal* reported last week that operational information for the Joint Strike Fighter, our advanced, stealth-capable, tactical air fighter was breached making it easier for enemies to defend against it if not to steal some of the highly classified systems within it.

We know that there are severe vulnerabilities in our electricity grid and that foreign governments seeking to map our infrastructures have intruded into our electricity systems on a very large scale.

So there is all too much evidence that our cyber infrastructure is insecure and, unfortunately, there is a lot of evidence that our security capabilities are inadequate to the challenge. GAO and various inspectors general have been repeatedly reporting on these weaknesses. Last December, the Center for Strategic and International Studies (CSIS) issued a report listing a vulnerability of cyber networks as one of our Nation's major security vulnerabilities, risks.

Let me focus just for a moment, for the record, on the Department of Homeland Security.

The cyber security authorities of the Department of Homeland Security are not just general under the rubric of Homeland Security, but they are clearly outlined in statute and presidential directives. Title 2 of the Homeland Security Act directs DHS to lead critical infrastructure protection efforts, which by definition includes cyber security. Critical infrastructure was defined in that act as "systems and assets, whether physical or virtual, so vital to the United States that the capacity or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of these matters."

In 2003, President Bush released a national strategy to secure cyberspace, which stated that the Department of Homeland Security would be "the focal point for the Federal Government to manage cyber security." Later that year, the White House issued Homeland Security Presidential Directive 7 (HSPD–7) to implement the critical infrastructure responsibilities laid out in the Homeland Security Act. HSPD–7 reinforced the leadership role of the Department of Homeland Security on cyber security, stating, "The Secretary of Homeland Security will continue to maintain an organization to serve as a focal point for the security of cyberspace."

In 2008, President Bush issued Homeland Security Presidential Directive 23 (HSPD–23) to implement the Comprehensive National Cyber Security Initiative, which focused on the protection of Federal networks. The exact language used in HSPD–23 is classified. However, I can say that the directive affirmed that the Department of Homeland Security serves as the lead Federal agency for the protection of Federal civilian networks, that is to say all unclassified networks, and for coordinating private sector cyber security efforts.

So as we come to this transitional point, we on this Committee feel strongly that the Department of Homeland Security has, under statute and presidential directive, a central and critically important role to play. And this Committee, in a sense, is here to ask you how you think DHS has carried out that responsibility—I know you will testify and much else—and also what we can do to help DHS do the better job that we all acknowledge we needed to do.

Thank you very much for being here. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

The information and communication networks that we refer to as cyberspace have become critical to our economy, our national defense, and our homeland security. Yet, every week, we learn of more threats to our cyber infrastructure. The spector of our adversaries disrupting our telecommunications systems, shutting down our electric power, or freezing our financial markets is no longer the stuff of science fiction; rather, it is a very real possibility as thousands of cyber attacks are launched everyday.

For example, intelligence officials tell us that China and Russia have attempted to map the American electrical grid and have left behind software that could be activated later perhaps to disrupt or destroy components. The *Washington Post* has reported that hackers broke into the Pentagon's Joint Strike Fighter project and stole information. And last year, as the Chairman alluded to, cyber thieves secretly implanted circuitry into keypads sold to British supermarkets, which were then used to steal account information and personal identification numbers. As these numerous intrusions demonstrate, the cyber security threat is real, dangerous, and accelerating.

Today, this Committee will examine the practical issues of how the Federal Government should best be organized to counter this threat. An effective response to cyber threats will require coordination among law enforcement, intelligence agencies, and private owners of critical infrastructure. The Department of Homeland Security is the crucial nexus of these realms.

Bringing together these three worlds is precisely the reason that Congress created DHS following the terrorist attacks of September 11, 2001. The Comprehensive National Cyber Security Initiative, started last January—and the Chairman referred to it—recognized the value of the Department's unique perspective by placing the National Cyber Security Center at DHS and charging the Department with the responsibility for advancing coordination and consultation among the many Federal entities with cyber security missions. And following up on this directive, last year, Senator Lieberman and I introduced a homeland security reauthorization bill that included cyber security provisions that would have increased the responsibilities of the center at DHS.

We also need to determine what specific authorities are necessary for DHS to undertake the mission of better securing Federal networks and our Nation's critical cyber infrastructure as the Department works with but does not supplant the important roles played by the Department of Defense, the intelligence community, Federal law enforcement officials, and other agencies.

These authorities must allow DHS to address many of the most pressing cyber security issues, including how do you share critical infrastructure on threats and vulnerabilities, particularly with the private sector, since 85 percent of critical infrastructure is privately owned?

How do you encourage the adoption of best practices and standards not only across government but throughout our Nation's critical infrastructure?

How do we best generate a strategy that deters terrorists and hostile nation states from executing cyber attacks that potentially could devastate our critical infrastructure?

How do we best go after cyber criminals, not necessarily from other countries, but within our own country? Sometimes that part is overlooked as we discuss the threat.

How do we secure the supply chain to ensure that systems we purchase are free from malicious code?

And how do we best establish standards and performance metrics that can guide government procurement to encourage manufacturers to incorporate better security into their products for the benefit of both government and the public at large?

Finally, as we consider the reorganization of cyber security activities, I would note that this new Administration has shown a tendency to appoint special assistants and czars within the White House for virtually every important issue that we are confronting. While I understand the need to shine a spotlight on critical problems, the creation of numerous czars or special assistants usually leads to conflict, turf battles, and confusing lines of authority.

Moreover, Congress' ability to effectively oversee activities directed from the Executive Office of the President are severely limited. Typically, we cannot call upon those in the White House to come testify before us, and their budget requests are presented with very limited details. So the issue of reorganization of cyber security efforts necessarily involves the discussion of accountability and oversight by Congress as well. On an issue as pressing and as complex as cyber security, congressional oversight is critical to making real progress.

I look forward to exploring these issues with our witnesses today.

Mr. Chairman, you have assembled the top experts, and it is a pleasure to welcome back to the Committee, of course, Mr. Baker, who has been here many times. Thank you for holding this important hearing.

Chairman LIEBERMAN. Thanks, Senator Collins. And thanks for the very thoughtful statement. I appreciate it.

Stewart Baker, good to see you again. Welcome back. You graduated from line authority to elder statesman, at an early age.

STATEMENT OF HON. STEWART A. BAKER,[1] FORMER ASSISTANT SECRETARY OF HOMELAND SECURITY

Mr. BAKER. It is a pleasure to be home again. Thank you, Chairman Lieberman and Ranking Member Collins. It is also a pleasure to have graduated from DHS. I served on a commission once, and one of the old hands of the commission said, "Yes, they have brought back all the people who could not do the job to tell us why we should do the things they could not do." And in that spirit, I would like to talk a little bit about the cyberspace crisis that we face and what DHS should do about it.

You both have laid out the problem quite eloquently, and I will not try to repeat that. I would like to explain why I think this problem persists and continues to grow worse. And I will use an example that I have laid out in my testimony.

There was a fellow named Howard Crank, a Vietnam vet suffering from diabetes. At home, he got an Internet connection, and the world opened up to him. He could interact with the world. It was a wonderful thing for him, until, essentially, scam artists found him and induced him to mortgage his house twice, to max out his credit cards and to go into bankruptcy trying to recover the lottery proceeds he was told he had won.

Right up until that moment, I think he would have said the Internet had done a great thing for him, but interacting with the world, and having the world interact with him, turned out to be a disaster because not all of the world intended him well.

We are all in that position. We are all getting benefits today from hooking up to the Internet, from using Internet protocols. They are making our lives easier and they are making the delivery of services and goods cheaper. And yet, every time we hook up to the Internet and expand the reach of those networks to other parts of our lives, we are creating greater risks. And, at some point the ice could give way and we could be dropped into the lake and lose everything.

That is the greatest concern, but today we are not seeing any obvious harm to our networks or to our way of life, and that is what has led us to ignore the problem or to minimize the problem.

I think it is a tribute to both this Administration and to the last that we are finally beginning to look at the ways in which we can address this problem more seriously, and I would also like to give credit to Jim Lewis for the Center for Strategic and International

[1] The prepared statement of Mr. Baker appears in the Appendix on page 75.

Studies report which I think very profoundly raised all of the issues that have to be addressed if we are going to successfully defend ourselves in cyberspace.

That raises, then, as Senator Lieberman and Senator Collins both suggested, the question of how to organize ourselves to defend cyberspace. And here, I would like to draw on my experience. I realized as I was preparing for this hearing, that I have helped to start two of the last three cabinet departments created in the Federal Government. And I have served on a commission that recommended extensive organizational changes in the Federal Government.

If I had to do it over again, I am not sure I would do any of that. That's because there is a predictable pattern in the reorganization of government. You start with a failure. You say, this is not working. We should create another organization to solve the problem. And that organization, since you have just dreamed it up, does not have any flaws at all. It will do everything you want done, and much better than the obviously failed institution that you are looking at today.

When comparing an existing institution, where we have real failures, to an imaginary institution that has no flaws, the imaginary institution always looks better. Then, of course, once you actually try to start the imaginary organization, the imaginary organization discovers that it does not have a budget, it does not have staff, it does not have an executive secretary, it does not have a human relations department to begin hiring people. And pretty soon, that new institution is deep into a cycle of failure of its own, which then leads people to say, well, that is a failure. We should reorganize. Maybe we should have this new imaginary organization to do the job of the last imaginary organization.

I say that because I fear that the one recommendation of the CSIS report that I disagree with most strongly is the one that says, DHS is not doing everything it should. Consequently, we should dream up a new organization, a national cyberspace office that will perform all of the functions that DHS should be performing perfectly and is not performing perfectly.

That recourse to an imaginary organization, in my view, is precisely the problem with the CSIS report. We would be much better, in my view, fixing DHS, which, of course, was given many of these authorities when it was an imaginary organization and now is deep into the second cycle, where people find that it is not doing the job perfectly. We would be much better off building DHS's capability, something that has just begun, I think, seriously for the first time in the last year or two.

DHS has now launched on the job of building a genuinely strong cyber security office that can provide guidance across the government, provide services and detailed capabilities to the President. If they are given the opportunity to do that, they will succeed. If they are kicked aside because they cannot perform and have not performed every job that they have been given in the last 5 years, I think that we will be making the mistake that we made with other organizations where we have said, since we do not have a perfect job being done by the existing agencies, let's make up a new agency, and hand them the responsibility.

I do not think we want to be in a position 2 years from now looking at a new organization that has been created to carry out this mission in the Executive Office of the President and say, "Well, gee, they have just hired their staff. They have just begun to organize their budget. They have just determined who their executive secretary should be. And, so for 2 years, we have been treading water and there have been a lot of failures since then." That is a recipe for treading water and not for making improvements.

I think we would be better off if we took the capabilities that DHS has and funded them, provided the resources and the staff that DHS needs, and let DHS carry out its responsibilities under guidance from a very strong National Security Council that can provide the muscle in the interagency that is necessary to actually achieve coordination across the government.

Very briefly, I will also talk about the question of regulation. I think it is clear that some form of regulation is necessary in this area. No private sector agency can be expected to fend off State actors who are bent on infiltrating its network. We do not expect Bank of America to fight our wars for us, and if the bank finds itself on the front lines of a war, we should be providing assistance to them at the Federal level.

In fact, there is regulatory authority in many of these areas. The Gramm-Leach-Bliley Act requires the financial regulators to have substantial authorities over cyber security. The Federal Communications Commission (FCC) has provided, and certainly has substantial authority over, cyber security standards if they choose to use all of their authority. The Federal Energy Regulatory Commission (FERC) has some authority. What is probably missing is some coordination and what I would describe as nimbleness in responding to new threats. And that I think is something that DHS can do if it is given clear authority and clear—not authority; they have the authority. They need a mandate from the Administration, from the President, and perhaps from this Committee.

Thank you very much.

Chairman LIEBERMAN. Thanks, Mr. Baker. That was very interesting testimony, very helpful, and has a certain healthy degree of skepticism that comes with having had considerable governmental experience. It is a longer view, but it is one that is very valuable to us.

Next, we are going to hear from the previously mentioned and saluted James Lewis, Director and Senior Fellow, Technology and Public Policy Program at the Center for Strategic and International Studies, which did the report to which both Mr. Baker and I referred. Thanks for being here.

STATEMENT OF JAMES A. LEWIS,[1] DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thanks very much. And I thank the Committee for the opportunity to testify. And also, I applaud your efforts to try and deal with the new security challenges we face. I am so glad to be here.

[1] The prepared statement of Mr. Lewis appears in the Appendix on page 86.

To summarize the state of cyber security, our networks are vulnerable, our opponents are inventive and energetic, and we are disorganized. Many people have worked hard in recent years, but the United States is late and we are not doing enough.

As a Nation, we have been slow to realize how important cyberspace has become for economic and national security, and, therefore, slow to give it the priority it requires. The United States is being dragged down by weak cyber security, losing its edge in commerce, innovation, and defense. The problems we face, espionage, crime, and risk to critical infrastructure, will never go away, but they can be reduced by coordinated government action. Put bluntly, we need a comprehensive strategy and somebody in charge of it.

To date, the United States has been unable to produce either leadership or a strategy. The 1998 Presidential Directive 63 still shapes policy, but it was overly fond of czars. The 2003 national strategy to secure cyberspace was neutered by ideology and internal conflict. The 2008 Comprehensive National Cyber Security Initiative (CNCI) has some valuable elements, but it was not comprehensive. It was also hobbled by infighting, and it came far too late.

So in 2008, CSIS, as you have heard, put out a report that recommended a comprehensive national approach. We called for the creation of a strong White House cyber advisor with clear authorities and a comprehensive national strategy that would use all the tools of U.S. power, international engagement, military activity, economic policy and regulation. Our report contained other important recommendations that I am sure some of my fellow witnesses will mention, including the need for increased education, modernization of outdated laws and other activities.

While policy must be led from the White House, agencies must carry out implementation and operation activities. Operational responsibility for cyber security falls on three agencies: The National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and DHS. The previous Administration assigned DHS the lead role for cyber security, but this was beyond its competencies. DHS is not the agency to lead intelligence, military, diplomatic, or law enforcement efforts. This does not mean that DHS does not have an important role, and it is time for that agency to begin to perform it.

DHS is responsible for protecting critical infrastructure and for securing the civilian government networks. It is beginning to build the capabilities needed to carry out these missions, but this will require sustained investment in facilities, technology, and DHS's cyber workforce.

To date, cyber security at DHS does not have the resources it needs. DHS needs better technologies to secure civilian and government networks. The CNCI had a program named Einstein. Einstein is inadequate, whether it is Einstein 1, 2, or 3. Who knows? Maybe 4 will work. The real question is whether there is a way for DHS to work with NSA to secure all government networks. This is, of course, a sensitive topic. NSA has the capabilities. DHS has the responsibility. But there are compelling constitutional reasons for restricting NSA's role. However, it would be a serious error not to take advantage of NSA at a time when our government networks are under sustained and successful attack.

DHS might also want to reconsider some reorganization within the National Cyber Security Division (NCSD). Perhaps a first step would be to merge the U.S. Computer Emergency Readiness Team (US–CERT) and the national communications systems and its component into a single entity inside of NCSD.

DHS's cyber functions are part of its National Protection and Programs Directorate (NPPD). This directorate needs better plans to merge physical infrastructure and cyber infrastructure protection. The National Infrastructure Protection Plan is more like a dictionary than a plan. DHS needs short implementable plans on how to protect critical infrastructure and assure the delivery of critical services in the face of cyber attack.

As part of its critical infrastructure responsibilities, DHS is the Federal interface with critical infrastructure owners and operators. This is an important role, but the current partnerships are inadequate, and DHS might want to look at the Department of Defense (DOD) Defense Industrial Base Initiative as a model for partnership and information sharing.

DHS must be part of the larger regulatory effort to improve cyber security. To date, the United States has relied on market forces and voluntary action. But to quote the former chairman of the Securities and Exchange Commission, "The last 6 months have made it abundantly clear that voluntary regulation does not work." Much of the opposition to regulation involves the replay of warmed-over dot-com ideology and a strong desire by the private sector to escape liability. I am very sympathetic to that.

As with any complex issue, there is no black or white answer. Too much regulation will damage the economy. Too little regulation will damage the economy and also harm national security. We need to find a middle course that balances commercial and national security interests. A new Federal approach to cyber security must elicit action from the private sector that it will not otherwise perform.

DHS does not have the regulatory authority for most critical infrastructure when it comes to cyberspace. One thing to consider is whether to give DHS new and expansive authorities or whether to use existing authorities with current regulatory agencies, like the FCC, FERC, Nuclear Regulatory Commission (NRC), Federal Deposit Insurance Corporation (FDIC), and there are many others.

The Administration has recently concluded a 60-day review of cyber security policy. This was a spectacular effort. Most of us did not think they would be able to finish on time. And while few public details have been released, it appears that the White House will play a greater role in organizing and leading cyber security policy. There will be greater attention to international engagement and to relations with the private sector, and there will be closer coordination among agencies.

My hope is that the 60-day review leads to a strong White House cyber advisor with clear authority to set policy and guide budgets. More fumbling among agencies will only lead to disaster. But with so many different equities involved in cyber security, we face gridlock. There is a regrettable debate over how much authority the

White House cyber advisor should have over policy and how strenuously the United States should protect its cyber networks. There is a trade off, some say, between security and innovation. I say this debate is regrettable because our opponents are not waiting 60 days to attack us.

The United States is in a very unfortunate situation. We have made better use of cyberspace than our competitors, and this has provided real economic benefits. Our reliance on cyberspace holds the potential for innovation and future growth. However, the combination of greater reliance and inadequate attention to security has left us more vulnerable than our opponents. If we cannot change this, the power and influence of the United States will shrink, and our prosperity and security will be damaged. Congress and the Executive Branch have the opportunity to avert this damage if we can act decisively.

I thank you for the opportunity to testify. I will be happy to take your questions. Let me say, it was more fun to testify against Mr. Baker when he was in the government because he was a little more constrained, but I welcome the opportunity to take your questions.

Chairman LIEBERMAN. Thank you.

Well, we like Mr. Baker in both roles. He is more unpredictable in this one. Both of you, though, have portrayed a crisis, which this is. And the question is what we can do together about it. Thanks for your testimony

Next, we are going to hear from Alan Paller, Director of Research at the SANS Institute.

Thanks so very much for being here.

STATEMENT OF ALAN PALLER,[1] DIRECTOR OF RESEARCH, SANS INSTITUTE

Mr. PALLER. Good morning, Senator Lieberman, Senator Collins, Senator Carper, and Senator Landrieu. Your taking on this issue is really impressive. It is a complex issue. The language is arcane. It is just a pain.

It turns out that you in your opening statement talked about what is really the central problem, which is that there is a gap between the attackers and our defenses. What is problematic is that the gap is growing at an increasing rate. So all this discussion is important, but we are falling behind at an increasing rate.

Let me give you just one simple example. There is a young man named Tan Dailin, who is a graduate student at Sichuan University. In 2005, the People's Liberation Army (PLA) noticed he was hacking into a computer in Japan, so they picked him up and said, wouldn't you like to be a contestant in our annual competition for who the best hackers are in Chengdu province? That is a southwest province of China.

He entered the competition. His team actually won 10,000 Renminbi. They put him through a 30-day, 16 hour a day, workshop, where he learned to develop really high-end attacks and tuned his skills. And then they put him in competition with teams from all of the rest of the military sub-units in the Southwest

[1] The prepared statement of Mr. Paller appears in the Appendix on page 90.

China, and his team won that. They won 20,000 Renminbi. He was famous and important.

He set up a little company. No one is exactly sure where all the money came from. But that company created the hacks that were found inside—this was September 2005 when he won it. By December, he was found well inside DOD computers. The summer of 2006 was a particularly bad summer for the United States because there were a lot of what are called zero-day attacks, which are attacks that happened using vulnerabilities that the vendor has not patched yet. So there is no defense. And his team was found to have been the team that built six of those 30 or so zero-day vulnerabilities.

What I am trying to say is that other nations are investing heavily in creating massive new technologies, and our defenses are childlike. What we have done under the Federal Information Security Management Act (FISMA) regulations is just embarrassing. And the result is much more than the public knows. You have not, but the House has had testimony saying the Commerce Department and the State Department have been deeply penetrated. What has not been told is that every other major department has been equally or more deeply penetrated, one so greatly that NSA had to bring their blue teams in just to find all of the problems.

We do not tell the public that because it is embarrassing, but it is just a symptom of what is happening. Eastern Europe has organized crime groups that recruit developers. But the way they recruit them is with lies and money. And then when they find out that they are working for organized crime, and they do not want to, crime groups use terror. They threaten their families. They kill their families if they do not want to work.

You talked about the $10 million that was obtained in 30 minutes. What was interesting about that case is the reason it stopped was the ATMs ran out of money. That was the only reason—they were just empty.

Chairman LIEBERMAN. Just take a moment and explain why the 30 minutes. Was that thought to be a period of vulnerability in the systems?

Mr. PALLER. Well, I did not talk to them. The FBI thinks they assumed they would not get caught doing it if it was short enough; that the triggers would not happen. What was fascinating is you might ask, how can they get that much money out?

The attackers actually had control of the computers inside the bank and were raising the limits of how much each of the cards could take out of the ATM as the ATMs were being emptied. You normally have a $300 or $500 limit. Those limits just kept growing, and it was because the attackers had control of the computers as well as they had made all these white plastic cards. But that $10 million is one of thousands of attacks.

You heard about the multi-city power outage that the hackers did. Why did they do that? Well, it is all extortion. If I have control of your computers, and I say I am going to take the power out, and you say, no, you will not, well, all I have to do is take the power out for 2 days, and every other utility will pay. It is a massive money-making scheme, and that money can be used to buy extremely advanced technologies. Our defenses, the way we have built them under the FISMA legislation are just—they are antagonistic to improve security. They are not just not improving security, they are actually working against it.

But there is a wonderful story I want to share with you. It is why I was happy to come today. It is one huge success. It is a Federal success. It shows not only can the Federal Government radically improve security, but that the effect can spill over into the defense industrial base and into the critical infrastructure.

It started when NSA was briefing John Gilligan, who is the Chief Information Officer (CIO) at the Air Force, and they told him they could get into Air Force systems in 30 minutes. And he said to them, you are not helping us. Tony Sager was the briefer from NSA. John said to Tony, "You are just not helping us. You show us how you break in. We fix everything. A few months later you are going to come in and break in again." This is the key statement. "Can you get all your attackers together and tell us what the critical things are we should have done that we should do to protect ourselves?"

You hear Melissa Hathaway talking about offense must inform defense. The fundamental error under FISMA was that we asked the people who did not know about offense to tell us how to do defense. You cannot do that. You just cannot do that.

So Tony went back and got the attackers together, showed John how to configure the systems, and they implemented those better configurations on a half a million computers, but they had to—this is from your opening statement, Senator Collins. You talked about the key role that the private sector plays using procurement. That is the one huge lever you have. There is nothing close to it. If you want to change security, the lever you have is procurement.

So what John did is he went to Microsoft. Microsoft said, no, we are not going to give you a different configuration than what we give everybody else. One size fits all. You have to take the one we give you. And he went to Steve Ballmer and talked him into giving them a more secure configuration. They implemented across a half a million machines. Here are the results.

One, it used to take 57 days on average to patch the machines. That is a good number in the Federal Government, 57 days, way too long. Now it is 72 hours and heading down toward 24. So they were able to change the way they manage computers because they have these good configurations. They saved $100 million in procurement. They save more than $100 million every year because they do not have to test the patches on every one of their different configurations. And they save $30 million on energy costs because the settings actually were energy-saving settings.

But most importantly, because all the experts said this would not happen, the users were significantly happier. The help desk director at the Air Force reported that their help desk calls were down by 50 percent because the users actually were better off. So here you have much better security, much lower costs, and happier users. And Karen Evans, to her credit, actually took that initiative and said to the rest of the government, let's do that as a government.

The challenge right now is that the attackers have gotten so far ahead, that is only one piece of what has to be done. So John went back to Tony and said, what are the rest of the things that have to be done, and he has created a new list of the critical things that must be done to secure Federal systems.

The one most important thing in all of that lesson is, the Federal Government has the big lever. And it is the $70 billion in information technology (IT) procurement that you use each year. When we talk about a public-private partnerships, those are endless meetings. I am sure you have sat in on some of them. They go completely different, if you are about to spend a half a billion dollars, which is what John Gilligan did.

The great partnership is: Let's spend little pieces of that money—I am not saying increase the money. These commercial organizations are more than willing to deliver more secure systems. They actually like it, if you will tell them what secure is. That is where NSA comes in. You cannot ask the National Institute of Standards and Technology (NIST) to do it. They do not know what the attacks are. You have to get it from NSA and US–CERT.

But once you know what the defenses should be, you can use procurement dollars to actually spend less money and have more secure systems. And what I like most about that story is that it trickled down. Microsoft now sells that more secure configuration to the defense industrial base, to the utilities. So you, using your procurement power, actually changed the nature of software and hardware so that it has been built more securely, there is nothing to stop the venders from selling that more secure version to everyone.

So the idea of leadership to me is not whether it is a White House or DHS leadership, it is whether you use the $70 billion a year that you spend on information technology to make the Nation safer. Thanks.

Chairman LIEBERMAN. Thanks very much, Mr. Paller. That was really riveting testimony. And it is very important to tell these stories to help laypeople, if you will, get into this.

We will enter your statement, along with everybody else's statement, into the record. Also, please take a moment to tell us what the SANS Institute is and, therefore, what credibility you bring to this task.

Mr. PALLER. We are the main teachers. We have about 100,000 alumni in 60 countries. We train the FBI, the NSA, the British, the Japanese, and the Indonesians. We teach the very advanced cyber security courses, forensics, and intrusion detection. And we also run the Internet Storm Center, which is an early warning system.

Chairman LIEBERMAN. That is great. Thank you.

Tom Kellermann is the Vice President of Security Awareness, a pretty good title, for Core Security Technologies. He brings another unique perspective to assist the Committee as we undertake this responsibility. So we thank you for being here and welcome your testimony now.

STATEMENT OF TOM KELLERMANN,[1] VICE PRESIDENT OF SECURITY AWARENESS, CORE SECURITY TECHNOLOGIES

Mr. KELLERMANN. Thank you, Senator. I greatly appreciate the opportunity to debrief this Committee on serious economic and national security risks that we are facing today from a cyber perspective. Much of my experience comes from my days at the World Bank Treasury on the security team there. And I will caveat that with the need for all of us to appreciate the *Art of War* by Sun Tzu. We need to really appreciate how offense informs defense, but not only that, how we can better layer security and implement policies and programs to create defense in depth across not just the Federal Government but critical infrastructures.

The horrible events of September 11, 2001, should have taught us a fundamental lesson, which was that non-state actors will use technology against our critical infrastructures. More importantly, it is obvious since September 11, 2001, that terrorists' financing has been directly related to the proceeds of cyber crime, and the modern day silk road directly relates to those bank accounts that were pilfered in that case that Melissa Hathaway spoke of at RSA Security.

The DHS has done a successful job, I think, regarding increasing the Federal standing per cyber attacks, however, there are some challenges that do detract from these efforts. First of all, the lack of management continuity. Many of DHS's senior cyber security leadership positions are political appointments by nature, and they result in frequent turnover of management personnel and changes in priorities and focus of an organization's mission. There is an insufficient support structure within DHS to provide fundamental functions to support cyber security needs, particularly the needs of what I consider the four most functional aspects of the National Cyber Security Division, which are the Electronic Crimes Task Force, the Secret Service, the US–CERT, and the Federal Network Security Branch.

Specifically, as I relate to this, the Federal Network Security Branch is no longer the lead when it comes to establishing the standards of cyber security and computing across civilian agencies, and many times it has to defer to the Office of Management and Budget (OMB). So that leadership position should be increased. I think that they should have the capacity to conduct red-teaming exercises against civilian agencies to determine where these vulnerabilities are, to determine where the priorities should be for IT spending.

This is a common problem across the Federal Government, where you have CIOs and Chief Technology Officers (CTOs) leading the way vis-a-vis what should be spent on IT and IT security. And CIOs' mind-sets are much about productivity, efficiency, access to services, and culturally differ from the defensive perspective of Chief Information Security Officer (CISO) community. And I think that it is important from a governance perspective that the perspective be raised to the top, particularly vis-a-vis the allocation of budgets and the expenditures of funds necessary to secure systems.

[1] The prepared statement of Mr. Kellermann appears in the Appendix on page 100.

To this point, as evidenced by specific campaigns carried out against Federal agencies in recent years and further illustrated by recent trends emerging in the larger cyber crime landscape, a true lack of situational awareness and an inability to predict the specific methods being utilized by electronic assailants is pervasive throughout the Federal Government, particularly as it relates to the recognition that the enemy no longer wants to disrupt service; the enemy wants to remain persistent and clandestine. The enemy in fact wants to launch a cyber insurgency or a cyber infiltration against your systems. And in the end, if they are given command and control, they want to remain on mission but also be able to control the integrity of your data to manipulate you in any which way they should feel necessary.

To address this dire reality, which has been highlighted most recently by the publicly incidence of energy hacking across the grid, not only in the U.S but overseas, and the Heartland payment systems breach, which was one of the most massive financial breaches in the past 50 years—to that note, over 200 banks were impacted by the Heartland breach, not just the cards themselves, but those bank systems that were connected to those systems—we need to represent the reality here that cyberspace is an aquatic environment. And if you can attack one segment of the water, you can infect the entire environment.

It is important that because of this reality, the Federal Information Security Management Act compels agencies to undergo more frequent, internal assessments to gauge their risk to cyber attacks, and not just check-the-box exercises for compliance, but really using the dynamic guidance given that is being sponsored by Tony Sager and John Gilligan, vis-a-vis the Common Audit Guidelines (CAG). And, specifically, agencies should be required to conduct regularly extensive security audits of their IT systems using the red team mentality and best practice identified by folks like Tony Sager, John Gilligan, and the CAG.

In addition, I would ask this Committee to consider the creation of systems of accountability, including penalties for those organizations and civilian agencies who are not properly addressing those critical vulnerabilities, and tailoring their IT budgets to addressing those critical vulnerabilities. There is too much plausible deniability in the system right now, and people do not actually undergo this type of red teaming or penetration testing because they want to maintain plausible deniability to insulate themselves from not only the clean up but also the criminal negligence that would come had they not addressed or remediated the problems that were found.

In addition, we must use these benchmarks to extrapolate this phenomenon to third-party outsourcing. The infamous breach of DHS 3 years ago was based on a lack of a standard of care in due diligence enforced by a third-party managed service provider. The previously noted Verizon Data Breach report noted that 39 percent of breaches were directly related to strategic partners. This was not cases of strategic partners attacking systems, but those systems of the strategic partners being compromised and used as island hops to transit and attack those primary systems.

It is imperative that we grapple with this systemic risk imposed by the outsourcing and offshoring of not only American jobs but the digital ecosystem on which we are heavily dependent. In order to promote and create a secure U.S. cyber ecosystem, this Committee should consider mandating that all entities who provide managed information security services, of any sort to the U.S. Government, or providers of such services to critical infrastructures as defined by the National Infrastructure Protection Plan (NIPP), at the very least enter into information security service level agreements, which go beyond the service level agreements today, which are essentially contracts that have mediocre terms of liability and recourse and are far too much focused on resiliency and up time of the data versus the integrity and confidentiality of said data.

The agreements must require that these service providers, at a minimum, have the same standards of legal and layered security as defined by NIST–800–53, but also move forward and allow that entity, the primary consumer of those services, to conduct audits based on things like the CAG of those systems, and mandate remediation timetables of those systems.

We must use Federal acquisitions policy to require that these service providers comply with all these individual requirements. Those organizations who already are compliant with FISMA, who are being proactive, should inherently receive tax credits or some sort of benefit from the system for being good Samaritans in the cyber landscape.

In summary, while the national and worldwide cyber pandemic is currently scaling in an exponential manner, I would submit that the significant gains can be realized through the Federal Government today by the political obligation of more aggressive attention to these issues. In this dark hour, we need strong bipartisan leadership. The dramatic increase in cyber attacks necessitates action. The recent 60-day cyber review developed by Melissa Hathaway represents a great starting point for real policy and strategic leadership, but it cannot be operational without the good work of DHS and this Committee.

It is paramount that this Committee understand that it too can serve a fundamental role of change in defending our Nation's critical infrastructures from this pervasive phenomenon, and I appreciate your consideration of my statement and, of course, your public service.

Chairman LIEBERMAN. Thanks so much, Mr. Kellermann.

That sets it right up for the question period. We will do 7-minute rounds of questions.

Let me make a statement based on what you have said and what I have learned here on this Committee, but also in the Armed Services Committee. We have a lot of overlap between the two committees.

For a number of years, we have been warned in the Armed Services Committee of the threat of asymmetrical warfare, which is to say the United States has become so strong in what might be called conventional warfare that it would be natural for somebody wanting to do us ill to not try to compete with us on that level, but to look for the weakness, the vulnerability, and to attack us in that sense, asymmetrically.

The second reality that we are dealing with, of course, is that after September 11, 2001, we are involved with Islamist terrorists in a global conflict, in which some of the old, traditional rules of warfare are gone, which is to say, this is not planes against planes, ships against ships, armies against armies in conventional battlefields. People strike it as from the dark and have no hesitancy to strike civilian populations, as we saw here, painfully, on September 11, 2001.

So you put both those together, the warnings that we got about asymmetrical warfare and the new rules of the conflict we are in, particularly in which civilian targets are open targets, cyber attacks just jumps right out at you, doesn't it, as a major threat to the security of the United States; and makes relevant not just the defense that the Department of Defense must provide to defend cyber systems, but all of the privately controlled cyber systems in our country that really are in control of our financial system, our power generating system. You could go on and on; our healthcare system could be incapacitated.

So I want to invite a reaction. To me, this is a real crisis, but I invite you, if you think I am overstating it, to say that. But here is my concern. If I were an enemy, either a state enemy or a non-state enemy, like a terrorist group wanting to do us harm, it seems to me one of the first most attractive ways to attack us would be a cyber attack, both because of the difficulty of finding me, the enemy, but also of the tremendous damage I could do at this point in the status of our cyber defenses.

Is this true, Mr. Paller?

Mr. PALLER. I think you are absolutely right, but I do not think the time is yet, meaning I think right now it is easier to bring a bomb across the border and blow somebody up. And if you are going to do terror right now, that simply works.

As we strengthen the borders, as we make it harder and harder to do kinetic attacks, this kind of cyber attack will become the attack of choice. And the reason that it is such a challenge, that you have to act right now, is that asymmetric warfare means pre-establish and control. So when the Chinese or another Nation gets into a Senate committee computer, they do not get in to steal the data, they get in to steal the data and to leave something so that they can change information at critical moments.

Chairman LIEBERMAN. Correct.

Mr. PALLER. So it is now that we have to fix cyber security in government and the commercial sector because the war will come later that will be fought in cyberspace. But I do not think we are sitting here waiting for a new attack against the power plants of America in the next 6 months.

Chairman LIEBERMAN. OK. You in your testimony, Mr. Kellermann, made some references as to how these both come together. Organized criminal groups see an opportunity to hold up private entities for money by threatening cyber attack or actually carrying them out. You raised the question of whether that clearing of the $10 million from the ATMs, some of that money may have ended up or may have started with organized crime, maybe not, and terrorism usage. But in your written testimony, you used the example of the Bali bombings in 2002 as an example of a terrorist attack that was funded by cyber crime.

Just take a quick moment and tell us about that.

Mr. KELLERMANN. What is interesting about the Bali bomber, Imam Samudra, was that he not only financed the attack through credit card fraud and precipitated through cyber crime, but he wrote a manifesto of sorts while in an Indonesian prison, stressing that Jihad could best be waged by using the money of the infidels to finance the physical acts of terror against the infidels. And you will see actually a spike—and I am sure Mr. Paller can speak to this with Internet Storm Center. You have seen a spike since in the number of hacker attacks emanating out of Indonesia. There is a realization of sorts that this Robin Hood mentality, that the lack of resources that these communities traditionally have, can be acquired through cyber means because the financial sector is so porous and too over-reliant on perimeter defenses.

But more importantly, vis-a-vis the different types of non-state actors, you have a dark ages mentality now in the underground, where you literally have communities that are assisting other communities without ever meeting them, in a very ephemeral sense, and acquiring the weapons grade technologies to attack systems, whether or not they have computer skill sets, as well as the sale of systems that have already been compromised is widespread, as well as financial details in bank accounts and credit card numbers can be sold for $40 a pop in this system, to any actor, so long as they are not considered a ripper, which is someone who is untrustworthy, that they do not follow through with deals.

Chairman LIEBERMAN. I have very little time left, but I want to just draw out, Mr. Baker and Mr. Lewis, on the debate you have about how we should best organize to respond to this.

Am I right that both of you agree that the Department of Homeland Security should have primary responsibility for non-defense Federal Government computers and for the interaction between the Federal Government and the private sector in regard to cyber defenses? Is that right?

I want to say for the record that both are nodding affirmatively.

So let me understand. Mr. Lewis, you have been very clear. You think there ought to be an office in the White House to coordinate everybody involved, DHS, NSA, DOD, and others.

But, Mr. Baker, let me understand what you are suggesting. Do you think the Department of Homeland Security should play the overall governmental coordination role or that there is not really a need for one?

Mr. BAKER. Let me address that. There is a need for more coordination; there is no doubt about it. It would be my suggestion that what is needed is not just a coordinator. This is something that the National Security Council does all the time. They coordinate and resolve disputes between agencies, and they can lead agencies.

What they will need is support in actually identifying the precise steps that ought to be taken on an urgent basis, if necessary, the kind of day-to-day research into the problem and the response to the problem, the development of standards and regulatory approaches and procurement standards that we have been talking about here. Everyone recognizes there needs to be greater detail in the Administration of the actual cyber security enterprise, and the question is, should that be done at DHS or by some new agency that will be created in the Executive Office of the President. I would suggest that it ought to be done at DHS.

Chairman LIEBERMAN. You would prefer DHS. And insofar as the overall coordination, you would have that be done by someone working at the NSC or the HSC.

Mr. BAKER. There is no doubt there needs to be very strong presidential leadership, probably through the NSC on this. It is really a question of how you staff that leadership.

Chairman LIEBERMAN. Right. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Baker, let me resume where the Chairman left off.

When Senator Lieberman and I sat down to implement the recommendations of the 9/11 Commission back in 2006, we quickly realized that one of the Commission's recommendations having to do with the placement of the National Counterterrorism Center (NCTC), within the Executive Office of the President was not a good idea. And our concern is that it would have placed the NCTC largely beyond the reach of congressional oversight, and it also would have limited the personnel and budget that the center could have. And it also had implications for privacy concerns as well.

When I hear this debate today, it is very reminiscent of the debate over the placement of the NCTC. One of the issues that we want to avoid is stovepiping again, of having agencies that are not coordinated, that are also beyond the reach of congressional oversight.

I know that you followed that debate very closely. Do you see any lessons for us as we decide where the appropriate entity is to do this coordination in the decisions that were made back in 2006 with regard to the placement of the National Counterterrorism Center?

Mr. BAKER. I do, actually. And I did follow NCTC's implementation closely, both because of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism and because I knew the first two heads of the NCTC and worked with them closely at DHS.

I think that the NCTC is a success, and a success in part because it is not in the Executive Office of the President. It is not buffeted by whatever is on the President's plate that day. It can actually build institutions, take the long view, and approach problems with a bit more discipline than you can afford when you are trying to follow the ball in the Executive Office of the President.

It also has been able to develop a privacy agenda that I think has worked. The responsibility to report to Congress has worked out well for NCTC and I think for the insight of the Nation into its activities. And I would envision a similar role for DHS. That is to say, when I was at DHS, I saw NCTC in some respects as an extension of the NSC. They worked for the NSC. They were particularly responsive to the President's priorities, but because they were outside of the immediate battle rhythm, they could do it on a more disciplined, long-term planning basis. And that is something that I think DHS can do if the President and NSC choose to use them in that way.

Senator COLLINS. Thank you.

Mr. Lewis, I want to ask you a more fundamental question that came up in a discussion that the Chairman and I had last week on this issue.

If a hostile nation were to shoot missiles at our country's power plants and, thus, disabled our electrical grid, we would immediately recognize that as an act of war. And the United States would marshal all of its resources to counter that action. Yet, if a hostile nation used computers to achieve exactly the same result, a complete disruption of our electrical grid, it is not at all clear that our government would view that as an act of war, assuming we could identify who was behind the attack, which is a whole other issue and challenge in and of itself.

It is my understanding that the CSIS report has some specific recommendations to the President on identifying cyberspace as a vital asset, and sending a message to those who would attack us, using computers rather than missiles, that we would consider that to be an act of war.

Could you talk about that issue for us?

Mr. LEWIS. Sure, I would be happy to. And let me say that we approached this as a national security problem, and we thought cyber security should be treated the way we treat other national security problems, which is that many agencies have a role. No agency has the lead. And so, when you look at our foreign policy or our national security policy, it is Defense, State, and the intelligence community. And all of them are coordinated by the NSC. And we thought the same sort of approach is the only way you can fix cyber security.

So, for me, when I listen to Mr. Baker, NCTC is not a good model. Its mission is too narrow. DHS does not have the capabilities. We do not want DHS making the decision when something is an act of war or when it is not. That is properly given to the President. And that is the real issue, when is it an act of war?

This gets back to some of your earlier statements. The Chinese have missiles. They are pointed at our power plants or at Los Angeles, but they are not going to launch them. They are not going to launch them until they need to. The Chinese right now have an intelligence advantage that exploit all of our networks, including yours. And they probably have left something behind that when there is a crisis, they can launch, just like they can launch their missiles. So this is not something that we should be surprised at. People have always been targeting electrical systems. It is just now they have a new weapon to attack it.

Two issues, though. How do you determine who the attacker is? My guess right now is we only know perhaps in a quarter of the cases at best who is actually launching the attack. The other issue is when you decide to respond and how you respond.

A response does not necessarily have to be keyboard versus keyboard, and we usually think of it that way. There is some geek over in China and there is some geek over in the United States. We have to get away from that. We have to say, from the White House, cyberspace is a vital national asset and we will use all means to protect it. A simple statement like that would be very helpful in putting our enemies on notice.

We then have to follow it up with some actions. Again, for me that points to who should the lead role be. If you are going to expel an attache from an embassy because of a cyber incident, this is what you would normally do in espionage, it is not a decision that would be made by any one agency. It would be made by a couple of agencies working through the White House. So we have to start treating this like a grown-up national security problem and getting the real national security system involved.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Senator Landrieu, welcome.

OPENING STATEMENT OF SENATOR LANDRIEU

Senator LANDRIEU. Thank you. And I appreciate the leadership of this Committee in an area that I feel very strongly about as well. And our State has made some initial steps working with the Air Force, in particular, to establish some benchmarks on this effort, which is why I am here today and want to continue to be involved.

Before I ask my questions, Mr. Paller, let me ask what happened to the $10 million? Did they actually get it? Do we know where it is, and was it returned?

Mr. PALLER. The $10 million is in the hands of the organized crime group.

Senator LANDRIEU. And that is——

Mr. PALLER. It is gone.

Senator LANDRIEU. It is gone.

Mr. PALLER. And there are several more similar things happening as we speak, like that.

Senator LANDRIEU. I know the primary debate, and it is an important debate, is how this is coordinated between agencies and who might take the lead role, but you have been very clear that there will be many agencies involved.

Looking at the sectors that warrant the most protection, from the financial sector to the utilities sector, other sectors, and given, I think, Mr. Kellermann's comments about terrorists using our own financial sector and access to it to actually fund their operations, how would each of you rank those sectors in terms of importance, since we are behind?

If we had to rank in order of efforts to protect, what order of sectors do you think is most important?

Mr. Kellermann, why don't you go first?

Mr. KELLERMANN. I would say financial sector is actually most important because, right now, for the last 10 years, organized crime and non-state actor community in general has been feasting on financial fraud, whether it is personally identifying information or funds transfer out of systems, which is why there has been an 80 percent increase in wire transfer fraud this past year.

Senator LANDRIEU. And what would the second area or third area be?

Mr. KELLERMANN. I would think there needs to be much more attention, actually, being paid to the healthcare sector, considering that we are trying to digitize health records, which can all be used to establish lines of credit in the same fashion that financial data could, in order to have revenue streams, per se, coming from the developed world into the developing world. The energy sector is obviously very important, the Smart Grid. It is going to create a huge systemic and operational risk that needs to be dealt with, and security must not be retrofitted on that.

But realistically, the non-state actor community is using financial information and health information to establish lines of credit to finance physical acts of violence against U.S. interest. But more than likely, the state actors who have already penetrated these systems, they are not going to actually turn off the systems or change the integrity of the systems until there is actually an international conflict with the United States. So we can wait a little bit vis-a-vis those actors due to diplomacy and the need for the DOD to get their act together when it comes to cyber security and cyberspace.

Senator LANDRIEU. Would any of you like to add something about—go ahead, Mr. Paller.

Mr. PALLER. Two completely industrial sectors. I think the greatest losses we could have, the place we have to act most quickly is in the defense industrial base. When you hear about the military losing things, it was not the military; it was the contractors. Those firms advise government on how to secure our systems, and then, like shoemakers' children without shoes, they give up all of the data. It needs a lot of attention, and DOD, as Mr. Lewis discussed, is already trying to focus on that.

The second one for me is the power system. But I think the fact that he has two and I have two different ones means that you will find that the only way to fix those is through Federal procurement. If you do not enable them to buy more secure systems baked in, they are not going to be able to do it. You cannot fix the security of a system after you have bought it. If the people sell you a broken system, it is broken.

Mr. LEWIS. Just really quickly, we went through this in the commission, and we identified four sectors. The reason we identified them is we wanted to be able to take punches and keep moving, right? And those were the energy system, particularly, the electrical grid, telecommunications, finance, and government services, particularly at the Federal level.

If those four can keep operating in the face of attack, we will be able to continue to perform as a nation.

Senator LANDRIEU. Let me ask you, has the Pentagon identified which branch of the Armed Services should take the lead on this effort? Is it more natural to the Air Force or to the Army or to the Navy? If anyone would take 30 or 45 seconds to briefly describe your views on that.

Mr. LEWIS. The services all have different capabilities. I hear Navy is the best. Do not know that, but that is what I hear. DOD has decided to set up a new joint command with all the services, located at Fort Meade.

There is a question about where it will be. Right now, it is under Strategic Command (STRATCOM) It might become an independent one. But the decision appears to be no one service; create a joint command, and that is probably the right decision.

Senator LANDRIEU. Is there any role for the National Guard that any of you could foresee in this? And if you would like to describe or have you thought about that at all?

Mr. Paller.

Mr. PALLER. Definitely. The key is you need practitioner knowledge. I train the National Guard guys who go over to Iraq each summer. They are wonderful. They have a lot of experience there. They have the skills. So the merger of that skill set of technology-literate people with the military is one of the great assets we have.

Senator LANDRIEU. And it seems to me—and Mr. Chairman and Senator Collins, I want to particularly stress the idea of the National Guard taking a leadership role, and the idea that the kind of people that we need, Mr. Chairman, to man this command would be people that could be recruited from high levels of the private sector that might not be engaged 20 or 25 years in the Armed Services, but would be at very high levels that could be recruited to come into the National Guard, specifically committed to this mission.

So I would urge this Committee to look carefully into the role that they might play, being located in all the States, very close, of course, to the governors and to the State government, and a good nexus between the Federal and State government. That might be an opportunity.

I have many other questions I will ask. I only have 14 seconds. So in closing, in terms of education and training in either our colleges, universities, or other levels, could you maybe, Mr. Paller, since you are involved with the SANS Institute, give a quick response to what some of our education committees could be doing in terms of investing in the workforce necessary to create the kind of intellectual strength we need in the coming decade or two for this in our country, given that so many international students are here and then leave with these prerequisite degrees and go back to other countries, some of which are not friendly?

Mr. PALLER. Big question. I will just give you one quick answer, and I will give you more if you want it later. But the quick answer is the most important thing you can do is change the way computer science and computer programming is taught in America, because programmers are not taught to write secure code. Every single one of these attacks happens because of a programmer error, and we are not teaching the kids who write software to write software securely. The faculty does not want to do it. So if you want to fix something, that is a wonderful one to fix.

Mr. LEWIS. Just quickly on that one, the President's speech yesterday got it right when he said we have to re-focus on science, technology, engineering, and math; that we have underinvested since the end of the Cold War, and now we are behind. And so it was great to hear yesterday. That will help create the environment where Mr. Pallen sort of training can really flourish.

Mr. KELLERMANN. If I may, also I think that MBA students and MBA programs are very short-sighted because they teach that technology increases efficiencies and accessibility services, and productivity. They do not teach the risk management side of implementing widespread technology or the implications of systemic risk, whether it is outsourcing or offshoring. It is just looked at as a win-win and a panacea for fraud actually.

Chairman LIEBERMAN. Thanks, Senator Landrieu.

Senator Carper is next on the list, but he is in the anteroom in a meeting. So I am going to call on Senator Burris in a minute.

I want to express regret, apologies, to the four witnesses that I have to go off to another meeting. I believe Senator Landrieu and I are heading in the same direction. But we are going to leave you in the able hands of Senator Collins and Senator Burris, who will carry the hearing to the conclusion.

You have been an excellent panel of witnesses. The reward for this behavior is that we will undoubtedly call you back. Senator Collins and I both were briefed by Melissa Hathaway last Friday. And her report is with the President, so we expect some public announcement of this soon. The President has built on the increases that President Bush asked for some of the cyber defense initiatives, in the fiscal year 2010 budget. And I expect that we are going to want to take a very active role here, probably including a legislative role. So I thank you very much for a really helpful testimony.

With that, Acting Chairman Burris.

Senator BURRIS. Thank you.

Chairman LIEBERMAN. You have come a long way very quickly.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS [presiding]. Thank you, Mr. Chairman, and Ranking Member Collins, and for an excellent testimony from our distinguished panel.

One thing that is going through my mind, gentlemen, is a simple question. Mostly, it seems like we are on the defensive in all of this. We are doing all the planning to try to protect every aspect of our data from the would be hackers or skilled intruders.

Are we in this country doing anything on the offense? I mean, are we seeking to reach out to some of these would be entities and also trying to hack into them to figure out what is going on on their side?

Mr. Lewis, would you like to take a shot at that?

Mr. LEWIS. Sure. Let me start, and my colleagues can join in.

We have offensive capabilities. They are among the best in the world. The problem is what I would call asymmetric vulnerabilities. We are a target-rich environment. So even though we are as good as our opponents, they have more stuff to shoot at. So, yes, we have offensive capabilities, but we are not in a position where that really is enough to protect us right now.

Mr. BAKER. I would add to that. It is true. I once said that, in contrast to my experience at NSA in the early 1990s and my current experience in government, we have gone from a situation in the early 1990s where the score in the game might be one to nothing, sort of like a soccer game, today when it might be 187 to 149. The offense has just taken over the field.

Worse from our point of view, we are playing the rest of the world. We are on everybody's top five list as intelligence targets and they are all trying to get into our systems. And so for us to play defense, we really have to play defense against everybody else and that is a very demanding requirement.

Senator BURRIS. Now, you mean some of our friendly countries also or where they are so-called friendly——

Mr. BAKER. As Charles de Gaulle said, nations do not have friends; nations have interests.

Senator BURRIS. Well, the permanent interest arrangement, yes.

Mr. LEWIS. We have some good relations with some treaty allies, and then there is the rest of the world. That is a good way to think of it.

Senator BURRIS. And we have to try to protect our system from all of those entities that are trying to get in because we are the biggest person on the block, I assume.

Mr. LEWIS. We are the richest and the easiest.

Senator BURRIS. Which leads to the other question.

But to what extent are their turf problems that are being resolved in the various entities in these various systems that we are having? And I assume that you, Mr. Lewis, is saying that this should really be controlled by the White House and not by DHS.

Is turf a problem here in our security interests?

Mr. LEWIS. There are some really big elephants in the room. You have the Justice Department. You have the Department of Defense. You have the State Department. You have the intelligence community. These are hard agencies to control, and it is very difficult to get them all moving in the same direction unless you have somebody like the National Security Council kicking on them. And those of us who have been in the government know that you do not just tell the Attorney General or the Secretary of Defense and he does it. Someone has to have a reporting relationship, and the only place that exists is the President.

So, yes, there are huge turf battles. Those are not necessarily bad. It would be better if we had fewer turf battles, but the only way we will get there is by establishing clear White House leadership.

Senator BURRIS. I am pretty sure we do not put all our eggs in one basket, in terms of that would be a security problem if that were to happen.

Mr. LEWIS. That is right.

Senator BURRIS. But there is a concern of coordinating all of this various defensive mechanism, which seems to be a major problem for us to do.

Mr. LEWIS. I think the place where we have had a little confusion is the distinction between direction and an operational role. Nobody wants an operational White House, meaning in a battle, the general does not drive the tank, but the tank driver does not set the policies. We need somebody in charge, but the people who actually implement the policies, who carry them out, who have the day-to-day missions, that should clearly be at the agencies, particularly DHS, which has a very major set of roles here. But none of the individual agencies are going to be able to coordinate all the other players on the team, and we have to think of this as a team effort.

Senator BURRIS. Are you saying, Mr. Lewis, that DHS is probably the one that could look at setting the possibly policy rules for the other agencies, and there would be some type of oversight on those policy rules?

Mr. LEWIS. Not as it is currently configured. And Mr. Baker might disagree with me. But if you are looking for strategic thinking, if you are looking for international engagement, if you are looking for intelligence activities, all of those are in other agencies outside of DHS. In fact, the most active agency has been the Department of Defense. They have the National Defense University. It has done a great deal of work on defining things like when is it an act of war, what is deterrence in cyberspace. The intellectual capital is not located in any one agency, and that is why we need to coordinate.

Mr. BAKER. I do not disagree with much of that. NSA, in particular, is a source of enormous expertise and anyone who wants to make policy in this area is going to have to rely very heavily on them. Because they are the attackers, they know what works and they can, therefore, inform the defenders. And there is no doubt there has to be leadership from the White House and someone within the White House who is clearly responsible and able to make decisions and to drive consensus on the part of the departments.

Where I think we may diverge is, I believe that DHS really should be staffing that person with respect to civilian agency and private sector coordination. I recognize that DHS has had growing pains for sure, and a lot of people would like to give up on it, but there is no other logical place to do this. In the last year, DHS has made real strides. They have great leadership now. And I think they are in a position to do much more than they have done over the last 3 or 4 years.

Senator BURRIS. My time has run out on this round. But one question I hope that each one of you can respond to very quickly, what can we in Congress do in reference to this?

Mr. Kellermann, you want to give it a——

Mr. KELLERMANN. I think it is very important that we empower DHS to conduct red-teaming exercises across civilian agencies and critical infrastructures so they can identify what is most vulnerable; to allocate IT resources to fix these problems, so we at least have a benchmark of where we are and where we need to go beyond the compliance exercises that currently exist today. As well, I think through acquisitions policy, we need to mandate and require that those who provide managed services that create the systemic risks, the aquatic risks in the system, should be contractually bound to a standard of care, which has not been established yet.

Senator BURRIS. Mr. Paller.

Mr. PALLER. The key lever you have is forcing the agencies to spend their money to buy security baked in. If you keep telling them to do security after they have bought technology that is broken, they are just not going to be able to do it. So you are a great weapon, and this is the one committee that can both set what needs to be done because you have wonderful people at DHS now working with NSA.

Senator BURRIS. Are you saying put the authority in DHS to deal with the other agencies?

Mr. PALLER. Yes. The authority that was missing in DHS is what everybody calls the red button. At DOD, when Defense Information Systems Agency (DISA) says you are doing a bad job of security, if the other group says tough, DISA can pull the plug.

Mr. PALLER. So if you want DHS to have the authority you are talking about, you have to be able to pull the plug on their computers. And that is something that Congress has not yet been willing to do.

Senator BURRIS. Mr. Lewis, any thought on that as well?

Mr. LEWIS. Sure. The three things that I think that only Congress can do, it can set priorities, it can modernize authorities, and it can provide the resources.

Let me talk just for a second on the first authority.

If some of us were in a classified briefing from DOD and they said, we are having an attack—this gets to your missile point—how do we respond? Is it Title 10, a military activity? Is it Title 50, an intelligence community activity? Or is it Title 3 or some other law enforcement activity?

Right now, it is not clear. There is a whole set of problems as to how you could make it clear. But when you look at the authorities for response or for defense, they were mainly written in the 1980s, and they are out of date.

Mr. BAKER. I agree with everything that has been said up to now and I would offer this perspective as well. No one is going to come to you and say "I have a turf fight; I would like you to take my side." Instead, every time changes in policy are made, someone's ox is going to be gored. And you are going to have business groups come to you, contractors who say "I lost the contract because I had too many breaches, but that was not fair"; or "My product was deemed insufficiently secure, so I did not get the contract and that is not fair"; or "they are regulating me too hard."

All of those things are complaints that you will hear, and I ask that you take them with a grain of salt and ask, how are we going to solve the problem if we listen to all those complaints?

Senator BURRIS. Again, I am way over my time. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you.

Welcome. Thank you each for joining us today. And thank you for your testimony today and your responses to our questions. Also thank you for helping to guide me, my staff, and others here in this Committee and the Subcommittee as we attempt to develop legislation that we hope is going to be helpful in addressing the concerns you all have been raising.

My staff tells me that each of you has had a chance to take a look at the bill that we will be introducing later today. As you may recall, it revamps the way that the Federal Government handles cyber security. We do so by creating a new office for cyberspace. We focus on actual security instead of paper compliance and strengthen security officers within agencies.

You just, in an indirect way, provided some answers to a question I have. What Senator Burris had just mentioned are some things we can do in the Congress to respond to these concerns. So some ideas of what we can do are embodied in the draft legislation that we expect to introduce later today.

Could we just go down the row, and start with Mr. Kellermann, and just share with us what do you think is good about the bill that we have prepared for introduction and what is not so good? And are there some areas in the legislation that need to be added?

Is there something that is missing that of which we should be mindful?

Mr. KELLERMANN. As you stated earlier, I think that elevation of the office is critical. Moving away from paper-based compliance exercises to more dynamic benchmarking is fundamental. And increasing accountability is also highly important and paramount to the success of this.

I would like to see, actually, an expansion of it to bring to bear the four critical infrastructures that we have identified in the commission report because of the systemic nature of this risk, because all of these players, even private, can contribute through a lack of layered security to the economic and national insecurity of the government of the United States and the American citizens.

Senator CARPER. Thank you. Mr. Paller, before you answer, let me just say, in our business, as Senator Collins and Senator Burris know, we are always reminded to be on message. And I just want to say you were really on message. You were as good as anybody I have seen and always brought us back to procurement.

Mr. PALLER. You have three elements of the bill that are wonderful. I happen to be up on them because one of the press people called me at 11 o'clock last night——

Senator CARPER. How convenient.

Mr. PALLER. How convenient; exactly.

But one is you have attack-based metrics in there, monitoring the things that actually block real attacks. What people have been doing in the name of FISMA is looking at everything in the world that might possibly be interesting in security, and they have not focused on the things that will actually block the known attacks. You also have continuous monitoring.

Under FISMA, the government has been looking every 3 years. How long do you think that look lasts after the guy leaves? So there is a continuous monitoring of the critical ones. And the third one you have is procurement, gently, but it is in there.

The challenge with the bill is that it also has a bunch of other nice things that people who do not want to do those three things will rely on. The bill is great. Whether OMB focuses on those three, and whether you help OMB focus on those three, is a big issue, but it is a wonderful bill.

Senator CARPER. Good. Thanks so much. And thanks for your help in crafting it. Mr. Lewis.

Mr. LEWIS. You can tell who the guru is because I did not get called by the press until this morning.

Senator CARPER. Well, they called me. I gave him Mr. Paller's number [Laughter.]

I asked him to wait to a little later in the evening. I said I think he is out, so maybe around 11 or 12 o'clock.

Mr. LEWIS. I think the bill is exactly right. It creates leadership. It moves to better metrics. It gets away from the paper-based approach. We desperately need to fix FISMA, so I really hope this bill goes through.

Senator CARPER. Thanks so much. Mr. Baker.

Mr. BAKER. I agree, FISMA is not working very well now, and any steps along the lines of the legislation that can focus the effort to improve security on real threats rather than moving paper would be useful.

Senator CARPER. Thank you.

Let me stick with this a little bit if we could. I recognize that cyberspace is not an issue that is strictly the responsibility of the private sector. It is not the responsibility of civilian agencies. It is not the responsibility of just the Department of Defense or the intelligence community.

Given that acknowledgment, what office should be responsible for ensuring that information is not only secure but free flowing and ensuring our expectations for privacy and civil liberties?

Mr. BAKER. In my view, there are really two agencies at the heart of this effort, the National Security Agency for the security of Defense Department systems and for bringing to bear the sophistication of attackers on the defensive effort, and the Department of Homeland Security which has defensive responsibilities, both for civilian and private sector networks.

There are plenty of other agencies that have enormously important roles to play, but we do not have enough experts to spread them evenly among those agencies. We need to begin building a cadre of real cyber security experts on the civilian side that can match what NSA can bring to bear in the defense side. And I think DHS is where that critical cadre of expertise should be.

Senator CARPER. All right. Thank you. Mr. Lewis.

Mr. LEWIS. This has to be a team effort, so I think there are many agencies, as Mr. Baker said. I would have added FBI as the third critical agency in your mix. But right now, as one of my colleagues says, it is like a kid's soccer team, a bunch of 7 year olds, here is the ball, they are all after it. The team needs a coach or a captain, and that is where I would say that your bill gets it exactly right.

Senator CARPER. All right. Thanks. Mr. Paller.

Mr. PALLER. I think Mr. Lewis said it fine.

Senator CARPER. All right. But you did not say it. No, I was just kidding.

Everyone has said what needs to be said, except for me, so I am going to say it again. But I appreciate your brevity.

Mr. Kellermann.

Mr. KELLERMANN. I would concur with those comments, but I would stress one important fact that I think has been lost, and that is the privacy debate. We cannot achieve privacy without cyber security. The privacy advocates for a long time now have stressed that cyber security somehow impacts privacy. Physical security and the use of technology does impact privacy. But, realistically, the government does not have monopoly on Big Brother anymore, and that is anyone who can hack. So I think it is important that the population respects your efforts in trying to preserve their privacy with these efforts to improve cyber security.

Senator CARPER. I am intrigued by other nations that are hacking into our system. I understand the motivation for kids, they do it for fun, the challenge. I can understand the motivation for criminal groups for the monetary gain. There is a lot of money at stake here and they have the ability to do it without going into a bank and robbing the bank, but still capture even more money. And I can understand the motivation of nations that are hostile to us, like terrorist groups that would like to bring us to our knees. I can see plenty of motivation there.

It is less obvious to me when I see a nation with whom we have diplomatic relations, have had for some time, a nation with whom we have a robust trade relationship, a nation that buys enormous amounts of our Treasury securities. For that nation to be so anxious to be able to infiltrate our systems and, potentially, to undermine our systems, talk to us about that motivation, if you would.

Mr. BAKER. I think there are two things that are worth saying about this. First, we should not assume that all of the attacks on our systems are on behalf of a nation-state. There is a kind of shadowy world here that is closer to Sir Francis Drake than to an official naval force. That is to say, people maybe protected by their government, encouraged by their government, rewarded by their government, but they are also free actors. And there is plenty of that going on in this world—digital privateers, if you will.

But it is also true that many nations that we would consider friendly want the best possible intelligence about what we plan to do because it has a direct effect on their national security. And so they consider it only prudent to try to extract as much information from our networks as they can get. That does not mean they intend to shut them down, but the difference between extracting information and shutting down the network is just a question of what you leave behind when you get out. So, we do see nations that we would consider friends in our networks for precisely that reason.

Senator CARPER. All right. Mr. Lewis.

Mr. LEWIS. We are moving to a more competitive international environment. And that means, in the Cold War, it was us versus them. Now it is a multi-player game. It is more like baseball where you have many teams, and these teams want to get that intelligence benefit.

For me, this is basically a spy story. Now, in particular, the Chinese and the Russians, they have been spying on us for decades. They found a new way. It is really cool. They are taking advantage of it. Does that mean they are not also planning to use this as a weapon in the event of a crisis? Well, of course, they are planning that. But their primary activity, the primary risk to national security now, lies in the espionage losses that we are suffering.

Senator CARPER. All right. Thank you. Mr. Paller.

Mr. PALLER. There is one more dimension of it, the economic dimension. They may be military friends, but they may be economic competitors. The head of the British Security Service (MI5) sent a letter to the presidents of the 300 largest companies in the United Kingdom, saying, if you are doing business with China, China is using exactly the same techniques to break into your computers, and your lawyers' computers, to take the data they need so they can negotiate from a position where they know more than you do.

I know it is true in the United States because the managing partner of one of the largest law firms was the first visitor in my new house, telling me the FBI had been in to say every single document of every one of the clients has been taken from the law firm's computers. So there is a massive economic dimension to this, in addition to the military intelligence dimension.

Senator CARPER. Thank you. Mr. Kellermann.

Mr. KELLERMANN. To that point, why even focus on research and development anymore when you can steal competitors' ideas and have competitor advantage in the marketplace? And realistically, why bother actually conducting espionage in the traditional sense, as Mr. Lewis stated, when one can remotely access systems and compromise systems?

Senator CARPER. All right. That is a lot to chew on, isn't it, colleagues? It is a lot to chew on. Thank you so much for being here today.

Senator BURRIS. Thank you, Senator. We are going to call on our Ranking Member, Senator Collins, to see if she has any questions or comments.

Senator Collins.

Senator COLLINS. Thank you, Senator. I do have a couple more questions and one comment.

Mr. Paller, you and I agree that the Federal Government has potentially enormous leverage to improve the security of IT purchases just using its purchasing power. I found very compelling the story that you told of a Federal official essentially begging the head of Microsoft to provide a more secure configuration.

Do you have any specific recommendations for us on how we can use the Federal purchasing power to require the incorporation of better computer security in the software and hardware that we are purchasing?

Mr. PALLER. There are two levels you can do it. One is the same level the Air Force is doing, which is to persuade the vendors to sell more secure versions of what they now sell. And the way you do that is by setting up a partnership between the vendor and DHS and NSA to agree on what that more secure configuration is.

Senator COLLINS. So to agree on standards?

Mr. PALLER. On standard configurations.

Senator COLLINS. Standard, yes.

Mr. PALLER. So that we can all buy a safer version. They will push back, saying "One size does not fit all." And the reality is, Microsoft sells one size of Windows to 100 million people. Oracle sells one size of its database to 100,000 people. They all sell one size. So the line "one size does not fit all" is just a lie.

But the more important opportunity for immediate action is every contract—so this is not just the contracts to buy the big stuff. But every contract should have three clauses, and I actually put them in my written testimony. I think Ms. Evans actually pushed them when she was at OMB. One is you have to make your software work on the secure configuration because if you sell me software that does not work on a secure configuration of Windows, I have to change Windows or not use your software.

Two is, you have to make sure that the 25 most critical programming errors are not in your software. And I do not remember the third one, but it is in the written statement.

Senator COLLINS. Thank you. Those are very helpful suggestions and ones that we should adopt.

Mr. Kellermann, you have done a lot of work and research in this area, so I want to bring up an issue we have not talked about today. And that is trafficking in counterfeit information technology products. That is a global and growing problem. And, of course, it is unfair, because it costs legitimate patent and copyright holders millions of dollars of losses each year. But also, it is a security issue because these inferior products are far more likely to contain security vulnerabilities, either inadvertently because they are sloppily done, or by design.

Do we need some sort of concerted global crack down on counterfeiting of IT products to help improve our security?

Mr. KELLERMANN. Yes, I believe we do. And I think the messaging behind that should be focused on the security aspects of that software. Even if it is pirated Microsoft operating system software, it will not be able to receive updates. And so it will persistently have vulnerabilities and holes in code. And be able to message that through the corporations and/or governments that are purchasing this type of software will be important for their understanding of the operational risks that they are taking by taking the short cut through the woods in this aspect.

Senator COLLINS. Thank you.

Mr. Lewis, I want to end my comments today by disagreeing with you on the record in your description of the National Counterterrorism Center (NCTC). Along with Senator Lieberman, I am the author of the law that created that center, so I know very well what the NCTC's responsibilities are. And as the law says, not only does the NCTC serve as the primary organization within the U.S. Government for analyzing and integrating all intelligence information, with the exception of domestic terrorists, but also it is specifically assigned the role of conducting strategic operational planning for counterterrorism activities with all the instruments of international power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among the various agencies.

Senator Lieberman and I were talking that we remember this debate very well because it was extremely contentious to give NCTC the lead role in strategic operational planning. And on this issue, the NCTC reports directly to the President so that the agency has the credibility needed to do the job.

Furthermore, I had my staff check this morning, after you responded that NCTC had a very narrow mission, to see whether in the new Administration the NCTC is still acting as the lead for all agencies on strategic operational planning. And, indeed, it is. In fact, more so in this new Administration.

So I just wanted to correct that for the record.

Mr. LEWIS. Could I add one thing?

Senator COLLINS. You certainly can.

Mr. LEWIS. You all have done great work, and now I want you to do it for cyber security.

Senator COLLINS. As do we. But my point is an entirely different point, which is looked at putting NCTC in the office of the President. That was the recommendation of the 9/11 Commission. And it was one of the few areas—I can only think of three of the dozens of recommendations—where we disagreed with the 9/11 Commission and made an informed and considered choice to put this center in the Office of the Director of National Intelligence (ODNI).

It was the right decision. It has been judged as success by virtually everyone. And I think we have to be really careful about creating a new office, as Senator Carper had suggested, within the office of the President for fear that we are going to diminish our ability to exercise congressional oversight. We cannot call the czars or the heads of offices within the Executive Office of the President before this Committee. We cannot. We have very little say over their budget.

So I think we have to proceed carefully. That is not to say that we are looking at DHS, as you implied, to make decisions on declaring war. Obviously, that is not the case. That, obviously, is something that the President would do with congressional input, of course. But I think we have to proceed carefully here to make sure that we do not create a whole new round of turf battles, inadequate congressional oversight, and unclear lines of authority.

So I think we need, definitely, to strengthen cyber security, and the question before this Committee is how best to do that. And I believe that DHS is the logical agency, given how much of cyber security is in the private sector, to coordinate that role. That does not mean diminishing the role of NSA or the Department of Defense. Those have vital roles, and the FBI, as well. But this is something that I think is going to be the subject of a lot of debate.

So, Mr. Chairman, I thank you for allowing me to have some final comments on this important issue. And congratulations on being the acting Chairman.

Senator BURRIS. Thank you, Madam Ranking Member.

Just before we adjourn this hearing, I just want to throw out something to this distinguished panel, because I am an old bank examiner, I am an old auditor. And I wondered if we could not come up with the old system of having two sets of books.

Remember that? I am just wondering if we could not have two sets of computer systems. We will let them hack into one system and get all the information they want.

Has that been processed or brought up?

Mr. LEWIS. It is an interesting question, and it has come up several times in the past. Physically, it is probably not possible.

Senator BURRIS. It is not possible. OK.

Mr. LEWIS. No. But, virtually, meaning you could have two different systems running on the same infrastructure, people are looking at that. It may not be possible, but it is certainly an idea that is in discussion now.

Senator BURRIS. Well, at least I am on time.

Senator COLLINS. Thank you.

Senator BURRIS. Thank you, Madam Chairman.

We want to thank the panel. And as you heard Chairman Lieberman say, I am pretty sure with your expertise, you will be back.

So we will let the witnesses know that the record will be open for 15 days in case witnesses or senators have additional questions or statements.

Last, I would like to say, at this time, the hearing is adjourned.

[Whereupon, at 11:55 a.m., the Committee was adjourned.]

CYBER ATTACKS: PROTECTING INDUSTRY AGAINST GROWING THREATS

MONDAY, SEPTEMBER 14, 2009

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

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman and Collins.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning, and welcome to this hearing, and thanks to our distinguished panel of witnesses and to all who are here this morning.

There is an old familiar saying that, "No good deed goes unpunished." The modern technological corollary of that could be, "No good invention goes unexploited for bad purposes."

And so, as we will discuss this morning, it is in the world of cyberspace, as enemies and criminals have used its increasingly dominant role in our lives to attack our businesses and our Federal, State, and local governments—indeed, in some senses to threaten the continuity of our society, at its worst.

It was only 40 years ago that the first two computers were connected into what is now the Internet. Now nearly the entire world is online. The Internet has led to a wonderful revolution in commerce, communications, entertainment, and finance that has added greater efficiency, productivity, convenience, and even pleasure to our lives and our enterprises.

But, again, it seems that no good invention goes unexploited for bad purposes. And that successful computer experiment 40 years ago that gave us this remarkably interconnected world has also given us a global wave of cyber crime that threatens our national security, our economic security, and in some direct senses the well-being of individual companies and individual Americans.

In a hearing last April, this Committee examined in detail the threats to national security brought on by terrorists, nation-states, common hackers, and cyber criminals.

We learned a lot at that hearing, for instance, that computers containing information on the joint strike fighter plane and on our electrical grid have been compromised, possibly giving our enemies information that could make our fighter planes more vulnerable and, at worst, plunge large sections of our society into darkness.

Today, we are going to focus on a new wave of cyber crime in the private sector that is hitting businesses of all sizes across our country and ask the question: What can be done by the public and private sectors to make commercial cyberspace more secure, especially for organizations that cannot afford to have large information technology (IT) staffs on the job 24/7? And this is where I am grateful to the witnesses for being here.

We will hear first from two witnesses from the private sector who will describe how real a problem cyber crime is and what the private sector is doing and can do about it, and then two witnesses from the Federal Government who will testify to what the public sector is doing and what more it can do about this problem.

Just to validate the reality of it, in one particular example that now is familiar to those who follow this issue, cyber criminals operating out of Eastern Europe stole millions of dollars from businesses and local governments by first sending a seemingly innocuous e-mail to an unsuspecting company comptroller or treasurer. The message contained either a virus or an Internet link that installs a tiny piece of computer code designed to steal passwords.

Then, using those passwords to gain entry to accounts, the crooks patiently siphon off amounts of money, and they are clever enough, often, to take them in amounts of less than $10,000, thus avoiding triggering a bank report under Federal anti-money-laundering requirements. Their methods are so sophisticated that the traffic often seems to be coming from an authorized computer—which could be a legitimate computer that has been commandeered by the cyber criminal—so the bank or the other financial institution does not really know that anything is amiss.

The money is then transferred to "money mules." It is amazing how that term "mules" turns up in a lot of our investigatory work here, including people who carry drugs or weapons across the border in different directions between the U.S. and Mexico. But these a money mules are people recruited to set up bank accounts the stolen money can be transferred to and who then forward the money to the cyber criminals. Some of these people may not even be aware that they are taking part in a crime. They are often recruited to become "local agents" handling cash transfers for what they believe to be a legitimate company.

The cyber gangs find these people over Internet job boards by advertising the chance to "make money from home" or by contacting people directly who have posted resumes on a legitimate job service. Once the money shows up in the accounts the mules have set up, they are given instructions on how to wire it to other accounts which are controlled by the cyber criminals.

Using this basic approach, we know that cyber criminals have stolen an awful lot of money, in cases we know $700,000 from a school district near Pittsburgh; at least $100,000 from a bank account of an electronics testing firm in Baton Rouge, Louisiana; and approximately $1.2 million from a Texas manufacturer. These, of course, are only a few examples of what I think can now accurately be described as a cyber crime wave.

In 2007, TJX Corporation—the parent company of T.J. Maxx and Marshall's—experienced a breach in its wireless networks during which up to 94 million credit and debit card numbers were put at risk of being used illegally.

In 2008, the Heartland Payment Systems—whose CEO, Robert Carr—is before us today—was targeted by hackers in an attack that compromised at least 130 million credit card accounts.

These are just the large intrusions we know about. A lot of these cyber attacks, from what I have learned, go undetected or unreported because the victims are frightened to report them, either for reasons of security or because they have been threatened, or, frankly, because they do not want it known that it happened.

This is a real problem that we have to work together to stop. Forty years ago, as I said at the outset of my statement, the Internet was a tiny island of interconnected university computers that was still just an interesting academic experiment.

Today the Internet is a vast global system—a kind of new strategic high ground that we call "cyberspace"—that we really must work together to secure just as any military commander would seize and attempt to secure the high ground of any battlefield on which they were engaged.

But securing cyberspace is in some senses more complicated, though not, at this moment at least, as physically dangerous to do since the Internet is so, by definition, limitless, certainly in space, and thus, security cannot be achieved by the government or the private sector acting alone, and in some senses it cannot be achieved easily by either or both acting together. But we have to figure out how to do better at this.

A public-private partnership to defend the integrity of cyberspace is now urgently essential. Together, business, government, and law enforcement throughout the world must come together to deter these attacks and bring these criminals to justice.

Our Committee is working on legislation to help to make this so, particularly to further define and strengthen the role of the Department of Homeland Security (DHS)—which, of course, is the central jurisdiction of the homeland security part of our Committee—to strengthen the role of DHS in protecting all of us in cyberspace. That is why I look forward to this hearing this morning as a way to help educate the Committee on how best we can produce legislation that will really have the desired effect.

As always, it has been a pleasure to work with the Ranking Member of this Committee, Senator Susan Collins of Maine, and I call on her now.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, as you indicated, we are living in a wondrous new age of global information, an era that is being shaped by digital technology, consumer demand, and amazing innovation.

It truly is a remarkable time. Today, without thinking much about it, we send pictures, words, and video over the Web in a matter of seconds. We have immediate, 24/7 access to each other, texting and talking over affordable wireless devices. Technology is transforming our culture, our economy, and our world.

While we enjoy its many benefits, and most people cannot imagine life without computer technology, we must also be aware of the risks and dangers posed by this new world.

As the Chairman has pointed out, for every communications advance, there is also the risk—indeed, almost the inevitability—that the technology will be misused and exploited. Indeed, experts estimate that cyber crime has cost our national economy nearly $8 billion in losses.

Protecting our cyberspace has become critically important. In the past 18 months, this Committee has held three hearings on the topic of cyber security. Each time, we confronted a new line of cyber crime or cyber attacks.

Newspaper headlines paint a troubling picture of the state of information technology security in this country. This past Friday, computer hacker Albert Gonzalez pleaded guilty to charges stemming from the theft of tens of millions of credit and debit card numbers from the computers of several major retailers, including T.J. Maxx, Marshall's, and Barnes & Noble.

According to authorities, this may not have been his only major cyber crime. In August, he was indicted for his alleged involvement in the largest credit and debit card data breach ever in our country. Data relating to more than 130 million credit and debit cards were stolen from a number of corporations, including Hannaford Brothers—a Maine-based supermarket chain—and Heartland Payment Systems, whose CEO is testifying before us today.

In July, the U.S. and South Korea endured a sizable denial of service attack against both government and privately owned systems. The attack—launched by an unknown attacker—used a massive "bot-net" of hijacked computers to disrupt six Federal agencies, the *Washington Post,* Nasdaq, and other targets.

Most recently, there has been a significant increase in organized cyber gangs stealing money from small and mid-sized companies. The Financial Crimes Enforcement Network reports that wire transfer fraud rose 58 percent in 2008, with businesses generally forced to swallow substantial losses that they can ill afford in the current economy.

Like the Chairman, I am particularly concerned about the impact of cyber crime on our small businesses that do not have the armies of technology security experts available to them that a large corporation may have.

These incidents—coupled with the attacks and crimes that we have discussed in our past hearings—should prompt the Federal Government to get organized and to make cyber security a high priority. Thankfully, there has not yet been a "cyber 9/11," but information technology vulnerabilities are regularly exploited to steal billions of dollars, disrupt government and business operations, and engage in acts of espionage, including the theft of business, personal, and government data. These incidents can be devastating to our national security, erode our economic foundations, and ruin personal lives.

We are awash in recommendations on how to better secure our information infrastructure. The Center for Strategic and International Studies (CSIS), the 60-Day White House Cyberspace Policy Review, and numerous academics and industry stakeholders have suggested numerous ways to improve cyber security. As these latest incidents underscore, however, the time has come for the government to move from simply planning and studying reports to taking effective action.

Comprehensive cyber security legislation must be a high priority for this Congress, and I know that it is a high priority for the Chairman and for me. The Department of Homeland Security is designated as the lead agency for cyber security, but we must ensure that it has more authority to effectively carry out its mission, and the Chairman and I are working on legislation that will do just that.

A couple of important points that we should be undertaking right now: We need to improve information sharing between the Federal Government and the private sector. After all, 85 percent of critical infrastructure is privately owned.

Second, if we encourage the adoption of best practices and standards across the government, and if we encourage, through using our procurement power, computer manufacturers to build better security into their products, that will benefit the private sector as well, because the government is such a large buyer.

I look forward to discussing how we can strengthen that public-private partnership to ensure the security of this vital engine of our economy. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, for that excellent statement. Again, thanks to the witnesses. Normally, Mr. Carr, we begin hearings of this kind with the governmental witnesses. I appreciate the cooperation of the governmental witnesses. We thought in telling this story it would be a good idea to start with a particular case—Heartland Payment Systems—and what the private sector is doing now, and then invite Mr. Merritt and Mr. Reitinger to respond.

So our first witness is Robert Carr, Chairman and Chief Executive Officer of Heartland Payment Systems, Inc. Thanks for being here, and please proceed with your statement.

TESTIMONY OF ROBERT O. CARR,[1] CHAIRMAN AND CHIEF EXECUTIVE OFFICER, HEARTLAND PAYMENT SYSTEMS, INC.

Mr. CARR. Thank you, Senator. Good morning, Chairman Lieberman and Ranking Member Collins. My name is Bob Carr, and I am the Chairman and CEO of Heartland.

Let me begin by thanking the Committee for this opportunity to appear today to share our lessons learned. I will talk about the steps we have taken and what more can and should be done to better protect our customers and the public from criminal hackers.

Our primary business is to provide payment card processing services to merchants. This involves facilitating the exchange of information and funding between merchants and cardholders' issuing banks. Heartland provides full-service electronic payment processing services for merchants, including clearing and settlement, merchant accounting, and support and risk management.

When a consumer's card is swiped at one of our merchants, we forward the authorization request through the card brand, such as

[1] The prepared statement of Mr. Carr appears in the Appendix on page 153.

Visa or MasterCard, to the issuing bank. We then send approval back to the merchant, allowing the purchase to be made. We receive payment from the issuer, pass it on to the merchant, and provide statements and accounting to the merchant. It is important to note that in the course of our payment processing business we do not receive cardholder Social Security numbers, addresses, or unencrypted personal identification number data.

We were founded in 1997, and have since grown from 25 employees to over 3,100 employees. As of December 31, 2008, we provided our bank card processing services to approximately 230,000 merchant locations in America. Our total bank card volume last year was almost $67 billion.

On January 20, 2009, we announced the discovery of a criminal breach of our payment systems environment. This attack involved malicious software. The malware appears to have allowed criminal access to in-transit payment card data during the transaction authorization process. This data is not required to be encrypted while in transit under current payment card industry guidelines.

We were pleased to hear the recent news about law enforcement's efforts to investigate and prosecute the individuals who make up the criminal syndicate that law enforcement believes is responsible for the Heartland breach and others like it. Albert Gonzalez, the alleged mastermind of attacks on TJX and other retailers, including Barnes & Noble, Office Max, and Dave & Buster's, has pled guilty to charges in a 19-count indictment. The charges include conspiracy, wire fraud, and aggravated identity theft. Mr. Gonzalez is also accused of having hacked into our system, as well as that of Hannaford Brothers, ATMs stationed at 7-Elevens, and two other national retailers. It is reported that he was part of a team with Eastern European criminals who have attacked a variety of U.S. companies. We appreciate the efforts law enforcement is making to stop these attacks and bring these criminals to justice.

This has been a difficult experience for me and the company. We have taken a financial charge of approximately $32 million just in the first 6 months of the year on forensics, legal work, and other related efforts. Unfortunately, the company is involved in inquiries, investigations, and litigation so I cannot address in more detail the specifics of the intrusion. But I now know that this industry needs to, and can, do more to be better protected against the ever more sophisticated methods used by these cyber criminals. I want to provide the Committee with some additional information about what Heartland is working on to try and prevent such intrusions in the future.

Let me note two key areas where Heartland is hard at work to enhance payment industry security.

First, industry and government can be better coordinated. The Financial Services Information Sharing Council and Analysis Center (FS–ISAC), led by Mr. Nelson, has been a great resource to a broad range of financial services companies facing cyber threats. However, we could benefit from greater focus on the payment processing industry. To address the needs of payment processors, we recently formed, within the FS–ISAC, the Payments Processing Information Sharing Council (PPISC). The PPISC provides a forum for sharing information about fraud, threats, vulnerabilities, risk mitigation, and best practices.

At the PPISC, we shared with the payment industry members the malware that we discovered had been used to victimize our company. We did this once I learned that criminals were using this malware to attack the entire industry. I believe that by sharing this with others, including our industry competitors, we can better respond to very organized attackers.

Second, as reflected in the indictments of Mr. Gonzalez, a *modus operandi* frequently used by these attackers is to attempt to steal payment card data while it is being transferred in the clear—meaning it was not encrypted at the time. It is clear to me that we can address this vulnerability, and our internal technology team is now developing a possible solution we call E3, or "end-to-end encryption." I believe it is critical we implement new technology, not just at Heartland but industry-wide. We, at Heartland, believe we are taking the necessary steps to do that.

Heartland is working to deploy E3 to render data unreadable to outsiders from the point of card swipe. We plan to use special point-of-sale terminals, with tamper-resistant security modules to protect cryptographic secrets. We also plan to use special tools in our processing network, hardware security modules, to protect the cryptography associated with the card data.

Our goal is to completely remove payment account numbers of credit and debit cards and magnetic stripe data so that they are never accessible in a usable format in the merchant or processor systems. This includes expiration date, service code, and other data. We are taking the necessary steps to implement this E3 solution, and I want to let the Committee know where our efforts stand.

First, we are working with various suppliers on the technology to make E3 a reality and more ubiquitous. We are hopeful these efforts will minimize the costs to merchants while not inconveniencing cardholders. This is critical to a more secure payment processing system. We are seeking partners who will not use encryption as an opportunity to unduly profit at our expense or the expense of our merchant customers.

Second, we believe this potential solution needs to be implemented on an industry-wide basis. We have been working with the Accredited Standards Committee X9 to seek adoption of a new standard to protect cardholder data in the electronic payments industry so all users can benefit from it. Ultimately, the Payment Card Industry Security Council must approve this standard, and we are hopeful it will do so.

Third, once the standards are established, we will need the card brands and other financial institutions to cooperate and be willing to implement on their side the encryption system our merchants are willing to use. We have been meeting with the card brands, and we hope we will be able to make progress on adoption by the card brands. However, without the cooperation of all of the card brands, some of the encrypted data would have to be decrypted—and thereby rendered less secure—prior to transmission to the card brands and their issuing banks. I am hopeful that each of the card brands will ultimately accept encrypted transactions from all payment processors.

We are working on these solutions, both technological and cooperative, because I don't want any one else in our industry or our customers or their customers—the consumers—to fall victim to these cyber criminals. The attacks we face in this country potentially can have substantial consequences, and we can learn from our experience. While we cannot eliminate the risk, we can make cyber theft more difficult. I look forward to continuing to work to beat these criminals and appreciate your help as we continue this battle.

I welcome any questions Members have about my testimony today.

Chairman LIEBERMAN. Thank you, Mr. Carr, for that opening statement.

Now we will hear from William Nelson, who is President and Chief Executive Officer of the Financial Services Information Sharing and Analysis Center, which I have learned is known commonly as FS–ISAC. Thanks, Mr. Nelson. I presume you will tell us a little bit about the history of the organization.

Mr. NELSON. Yes, I will start with that.

Chairman LIEBERMAN. Go right ahead.

TESTIMONY OF WILLIAM B. NELSON,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER

Mr. NELSON. Chairman Lieberman, Ranking Member Collins, my name is Bill Nelson, and I am the President and CEO of the FS–ISAC. I want to thank you for this opportunity to address the U.S. Senate Homeland Security and Governmental Affairs Committee on this very important issue.

The FS–ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After September 11, 2001, and in response to Homeland Security Presidential Directive 7 and the Homeland Security Act, the FS–ISAC expanded its role to encompass physical threats to our sector.

The FS–ISAC is a 501(c)6 nonprofit organization and is funded entirely by its membership firms through dues and by sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services organizations. Since that time the membership has expanded to over 4,100 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 40 trade associations representing the majority of the U.S. financial services sector.

The FS–ISAC works closely with various government agencies, including the U.S. Department of Treasury, the Department of Homeland Security, the Federal Reserve; our biggest partner in law enforcement, the U.S. Secret Service; the Federal Bureau of Investigation (FBI); the National Security Agency (NSA); Central In-

[1] The prepared statement of Mr. Nelson appears in the Appendix on page 160.

telligence Agency (CIA); State and local governments; and other government organizations.

The overall objective of the FS–ISAC is to protect the financial services sector against cyber and physical threats. It acts as a trusted third party that allows members to submit threat, vulnerability, and incident information in a trusted manner for the good of the financial services sector. I have provided a complete list of the FS–ISAC information-sharing services and activities in the written testimony. I would, however, like to mention six of them to give you an idea of how the FS–ISAC meets the information-sharing needs of its members.

First and foremost, we provide delivery of timely, relevant, and actionable cyber and physical e-mail alerts from various sources through our Security Operations Center (SOC). This SOC operation is staffed 24/7 in order to keep our membership apprised of the latest threats, incidents, and vulnerabilities. Obviously, the cyber criminal does not work on a 9 to 5 schedule, and we must be constantly vigilant to respond to their attacks.

Second, we have Subject Matter Expert committees consisting of volunteers of our member firms. They serve on committees that provide in-depth analyses of the risks to the sector and recommend mitigation and remediation strategies and tactics.

Third, member surveys allow members to request information regarding security best practices at other organizations. The results of these surveys are then shared with the entire membership.

Fourth, we hold regular bi-weekly threat information calls for members to discuss the latest threats, vulnerabilities, and incidents. And we frequently have guest speakers from government, law enforcement—like the U.S. Secret Service—and from other sectors that discuss risk-related subjects on these calls.

And, five, we conduct emergency conference calls to share information with the membership and solicit input and collaboration. Last year, we had three emergency calls related to cyber threats and two pertaining to physical incidents.

And, six, we routinely conduct online presentations and have a regional outreach program to educate small to medium-sized regional financial services firms on threats, risks, and best practices.

A key factor in all of these activities is trust, and the FS–ISAC works to facilitate development of trust between its members, with other organizations in our sector and with other sectors, and with government organizations, particularly the law enforcement and intelligence communities.

Next I would like to briefly mention some of the public-private sector response to the cyber crime issue. We have been working with law enforcement, financial regulators, and our members, and we do recognize that the criminal threat to both affected institutions and to consumer confidence, in particular, posed by these activities, and we are taking steps to address areas of concern.

I think the U.S. Secret Service commitment to the financial services sector has been tremendous. They provide classified briefings for us, and they actually have an assigned full-time employee to our sector.

Another example of a successful instance of government-financial services sector information sharing occurred on October 24 of this year when the FBI, FS–ISAC, and the National Automated Clearinghouse Association (NACHA)—a rulemaking body for the Automated Clearinghouse Network—in case you do not know what that is, if you have direct deposit, you participate in the Automated Clearinghouse Network (ACH). We released a joint bulletin concerning account takeover activities targeting business and corporate customers. And, Senator Lieberman, you got a lot of your information, I think, from that bulletin or from the *Washington Post* that got a hold of it.

The bulletin described the methods and tools employed in recent fraud activities against small to medium-sized businesses that have been reported to the FBI. FS–ISAC and NACHA subject matter expertise was applied to that FBI case information to identify the detailed threat detection and risk mitigation strategies for financial institutions and their business customers. At the same time, we preserved the ongoing integrity of those investigations.

The bulletin was distributed to the FS–ISAC, to its over 4,100 members and its 40 member associations, so we think we were able to reach tens of thousands of financial institutions. So we are pretty sure that the bulletin ultimately reached nearly every financial institution in the United States.

The FS–ISAC and NACHA developed a comprehensive list of recommendations to financial institutions to educate their business customers on the need to use online banking services in a secure manner. As a result of this bulletin, financial services firms and their business and corporate customers have become more aware of some of the online risks facing them and how to detect malicious and criminal activities.

The FS–ISAC also works closely with other key financial services industry groups to protect the industry and its customers against cyber threats. My written testimony details some of these efforts, but I would like to mention one in particular. This year, the American Bankers Association, the FS–ISAC, and the Financial Services Roundtable worked with the Federal Government's General Services Administration (GSA), the Internal Revenue Service (IRS), and the Social Security Administration (SSA) to develop a proposal for better ID assurance for online e-Government applications. The goal of this effort is to leverage the "Know Your Customer" requirements that banks, credit unions, and other financial services firms employ for ID proofing and turn that into a higher level of assurance for access to online government applications. The project is right now in its proposal phase at present and still requires a funding commitment and more definition around the business model and system architecture. However, it is a great example of how the public and private sector cooperation is beginning to progress in this important area of online ID assurance.

From a regulatory perspective, financial regulators are actively involved in developing regulations and supervisory guidance and conducting focused examinations of information security, vendor management, and business continuity controls at financial institutions and major service providers. There are nearly a dozen booklets covering these key cyber security and business continuity issues in the Federal Financial Institutions Examination Council (FFIEC) handbook.

For the last part of my testimony, I would like to cover six broad recommendations. One is the need to improve cyber crime law enforcement. I think our partners in the United States are doing a great job—the U.S. Secret Service, FBI, and others—but there needs to be better international collaboration in particular regarding investigations and prosecutions. Law enforcement in many cases knows the threat actors, but in some countries, the governments and law enforcement in those countries often protect the cyber criminal.

Another area is that private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers so the cumulative dollar value of the crime committed may be many times the threshold that has been established. I think there needs to be improved communication at the local level between financial services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action can be taken.

I would support Mr. Carr's recommendation also that there needs to be stronger authentication and encryption. Financial services firms, processors and regulators need to encourage smart use of encryption and stronger authentication.

We also need to improve financial institution information security programs through a flexible and dynamic approach to cyber security.

And the fourth recommendation I came up with in the testimony is to improve the public-private sector collaboration. We need to expand information sharing between government agencies and the financial services industry. As part of that, we also need to improve the Internet infrastructure and use Federal procurement power to improve the security of software and hardware and services. We would support the recommendation that Ranking Member Collins and Senator Lieberman have come up with.

And last is education. There needs to be more public-private sector collaboration to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices.

In conclusion, industry, law enforcement, regulators, and DHS have responded to cyber crime threats against financial services firms and businesses and consumers, but more work needs to be done, and we look forward to making continued progress against cyber threats to our Nation. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Nelson. Just a point of clarification. When you referred through your statement to physical threats as well as cyber threats as a focus of your organization, I think I know what you meant, but why don't you clarify it for us?

Mr. NELSON. Yes. During Hurricanes Ike and Katrina, we stood up operations to be responsive to our sector to make sure they were aware of what was happening. We got really good reports from DHS about where power outages were likely to occur. In fact, they have a great predictive model for that.

We were able to provide information through some of the credit card processors of where merchants were actually processing transactions, so we knew where food transactions, medicine, building supplies, and other types of key critical information, where those transactions were processed. We directed that to DHS and to other sources so they could allocate resources and send people in the right place to get what they needed.

Chairman LIEBERMAN. That is physical threat from a natural disaster. Do you also include in the category of physical threat protection of physical financial services information from physical terrorist attacks, not cyber attacks?

Mr. NELSON. Yes, we also prepare for physical terrorism. We have services that were actually purchased for that, too. If there is a physical attack, let us say, in London—the underground bombings from a few years ago, we did report that. The Mumbai attacks, we reported that within 15 minutes of them occurring. We did not know exactly what was happening, but we did push that information out immediately. So we did report on that.

Chairman LIEBERMAN. I will leave this in a minute, but what about actually working with the financial institution? A while ago there was a lot of concern post-September 11, 2001, that there might be an actual physical attack on Wall Street to create the obvious disruption that would exist. Is that something you get involved in? For instance, with an explosive, a suicide bomb, something of that kind.

Mr. NELSON. Yes, we would. If there is any intelligence about that potentially occurring, we may get that from the intelligence community. We have over 150 people in our sector cleared for secret clearance, and, actually we are looking at adding more for top secret clearance. So if there is some threat intelligence about a potential physical threat, we do pass that on. And if the attack does occur, we report that. And we have a Business Resilience Committee that works on that.

Chairman LIEBERMAN. How about preventively or proactively? Are you working with member organizations to encourage them or assist them in protecting themselves from physical attack of that kind?

Mr. NELSON. Yes, we do. We get reports, for instance, some of these—the protester threat, for instance, recently. There is a G–20 meeting coming up in Pittsburgh. We have put out a number of reports on that from a source that we have, an international source that we got information on it, the type of threat actors that may appear at it—some of them actually fairly dangerous. They are not all sitting there with non-violent type protests.

Chairman LIEBERMAN. Right.

Mr. NELSON. There have been violent attacks in some of these cases. So we have been able to report on that and provide best practices on how to deal with it.

Chairman LIEBERMAN. OK. Thanks. We will come back to that.

Michael Merritt is next, Assistant Director, Office of Investigations, U.S. Secret Service, which is now part of the Department of Homeland Security. Again, thanks for being here, Mr. Merritt. Thanks for what you do every day. I hope you will begin by explaining to anybody who is watching this why the Secret Service is involved in this field since generally the public sees you almost exclusively as protecting presidents, vice presidents, and other public officials.

TESTIMONY OF MICHAEL P. MERRITT,[1] ASSISTANT DIRECTOR, OFFICE OF INVESTIGATIONS, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MERRITT. I would be happy to. Good morning. Chairman Lieberman, Ranking Member Collins. Thank you for the opportunity to address this Committee on the Secret Service's role in investigating cyber and computer-related crimes.

While the Secret Service is perhaps best known for protecting our Nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of U.S. currency. As the original guardian of the Nation's financial payment system, the Secret Service has established a long history of protecting American consumers, industries, and financial institutions from fraud. Over the last 144 years, our investigative mission and statutory authority have expanded, and today the Secret Service is recognized worldwide for our expertise and innovative approaches to detecting, investigating, and preventing financial fraud.

In recent years, we have observed a significant increase in the quality, quantity, and complexity of cyber cases targeting financial institutions in the United States. With the advent of technology and the Internet, a transnational "cyber criminal" has emerged, resulting in a marked increase in cyber and computer-related crimes targeting private industry and other critical infrastructures. Current trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers resulting in data breaches affecting every sector of the American economy.

As the well-trained, well-equipped, and sophisticated cyber criminals continue to target the large corporations who have historically had more resources and assets in place to protect their networks, the less sophisticated cyber criminals continue their attacks against the small and medium-sized businesses that do not have the expertise in place to protect their data.

For example, in October 2007, the Secret Service identified a complex fraud scheme in which servers owned by a payroll company were compromised by a network intrusion. Subsequently, four debit card accounts belonging to a small Midwestern bank were compromised, distributed via the Internet, and used in a coordinated attack resulting in ATM withdrawals in excess of $5 million. The withdrawals involved 9,000 worldwide transactions in less than 2 days, and the small bank had to file for Chapter 11 bankruptcy protection.

Following the investigative leads generated in this case, we were able to prevent additional losses by notifying victim companies of the intrusion and compromise, often before the companies became aware of the illicit activity. For example, when we discovered that the computer network of a U.S. bank had been compromised, our prompt notification enabled the bank to significantly reduce its exposure and avoid potential losses exceeding $15 million. Based on these investigative efforts, the Secret Service identified 15 com-

[1] The prepared statement of Mr. Merritt appears in the Appendix on page 174.

promised financial institutions, $3 million in losses, 5,000 compromised accounts, and prevented more than $20 million in potential losses to U.S. financial institutions and consumers.

While cyber criminals operate in a world without borders, the law enforcement community does not. The multi-national, multi-jurisdictional nature of these cyber crime cases has increased in complexity and, accordingly, increased the time and resources needed for successful investigation and adjudication. The anonymity, level of collaboration among cyber criminals, and transnational nature of these crimes have raised both the intricacy of these cases and the level of potential harm.

To face the emerging threats posed by cyber criminals, we have adopted an innovative, multi-faceted approach. A central component of our capabilities for investigating cyber crime is the Electronic Crimes Special Agent Program. Today this program is comprised of 1,148 special agents deployed in 98 offices throughout the world who have received training in forensic identification and the preservation and retrieval of electronically stored evidence. They are among the most highly trained experts in law enforcement. Additionally, in partnership with the Department, the State of Alabama, and the Alabama District Attorneys Association, we have established the National Computer Forensics Institute. The goal of this facility is to provide State and local law enforcement, prosecutors, and judges with the necessary training, not only to understand cyber crime, but to respond to network intrusion incidents and to conduct electronic crime investigations. This program has been extremely successful, and since opening in May 2008, we have provided training to 564 State and local law enforcement officials representing over 300 agencies from 49 States and two U.S. territories.

As cyber cases continue to increase in size, scope, and depth, as an agency we are committed to sharing information and resources with our law enforcement partners, academia, and the private sector. To accomplish this, we have established 28 Electronic Crimes Task Forces (ECTFs), including the first international task force based in Rome, Italy. Currently, membership in our Electronic Crimes Task Forces include nearly 300 academic partners, over 2,100 international, domestic, Federal, State, and local law enforcement partners, and over 3,100 private sector partners. These partners, who range in scope from companies with less than 20 employees to Fortune 500 companies, enjoy the resources, expertise, and advanced research provided by the Electronic Crimes Task Forces international network.

In addition, the network that has been established by our ECTFs was instrumental in making the Secret Service's first Global Cyber Security Conference last month a resounding success. This 3-day conference was designed to share the latest information in investigative techniques used to combat cyber crime. The conference was attended by personnel from over 370 entities representing 11 countries.

In addition, to coordinate these investigations at the headquarters level, we have established the Cyber Intelligence Section to collect, analyze, and disseminate data in support of our cyber investigations and to generate new leads. The Cyber Intelligence Section has been instrumental in our success in infiltrating online cyber criminal networks.

One such infiltration allowed us to initiate and conduct a 3-year investigation that eventually led to the identification and indictment of 11 perpetrators from the United States, Eastern Europe, and Asia. This case involved the hacking of nine major U.S. retailers and the subsequent theft and sale of more than 40 million credit and debit card numbers, commonly referred to, as it has been in this forum, the TJX investigation. The total account loss associated with this investigation is still being assessed. However, one of the corporate victims has already reported expenses of nearly $200 million resulting from the intrusion.

As I have highlighted in my statement, the Secret Service has implemented a number of initiatives pertaining to cyber and computer-related crimes. Responding to the growth in these types of crimes and the level of sophistication these criminals employ demands an increasing amount of resources and greater collaboration. It is not a threat of the future. It is a challenge being faced by law enforcement today. Accordingly, we dedicate significant resources to increase awareness, educate the public, provide training for law enforcement partners, and improve investigative techniques. The Secret Service is committed to our mission of safeguarding the Nation's critical infrastructure and financial payment systems. We will continue to aggressively investigate cyber and computer-related crimes to protect consumers.

Chairman Lieberman and Ranking Member Collins, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the U.S. Secret Service, and I will be pleased to answer any questions you might have during this session.

Chairman LIEBERMAN. Thanks, Mr. Merritt. I must say I am encouraged and impressed by what you have told us about all that the Secret Service is doing. It is very good, both the outreach here within the country to the private sector and law enforcement, but also based on your very accurate statement that cyber criminals do not know boundaries but law enforcement authorities do; and, therefore, we have to create places and perhaps institutions where the good guys can figure out how to work across boundaries with the same speed and effect that the cyber criminals do. So I look forward to the question period.

Our final witness on the panel is Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate (NPPD) of the Department of Homeland Security. Mr. Reitinger, we welcome you here, and really welcome you to the Department generally, with a lot of enthusiasm and high expectations. The Department was created out of legislation from this Committee. We follow it closely. We feel good about a lot of the progress being made in the Department. I personally give the Department some good share of the credit for the fact that we have not suffered another major terrorist attack since September 11, 2001.

But it is my conclusion also—and I am not alone—that in this particular area of cyber security, the Department has not moved as quickly and as effectively as it should have. So your coming to this position is very important to a lot of us. Everything we know about you says you have the credentials and experience to do the job. So do not screw up. [Laughter.]

Chairman LIEBERMAN. Go ahead, Mr. Reitinger.

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

Mr. REITINGER. Thank you, Chairman Lieberman, Ranking Member Collins. It is indeed my commitment not to screw up.

It is an honor to be here today to talk with the Committee. This is my first opportunity to appear before Congress to testify specifically on cyber-related issues, and I am very pleased to be here today to do so.

I would like to start with the threat, if I might. I think the Committee, the panel, and the audience know that we are dealing with an increasingly dynamic and threatening environment in many ways. Hacker skill is rising across the board. Not only are the best hackers becoming better and better; "script kiddies," as we used to call them during my law enforcement days, increasingly have more and more sophisticated tools so that they can wreak a high degree of damage without even knowing too much about what they are doing. And relevant to the topic of information sharing, hackers in some ways remain better at information sharing than we, in government, have been. So that is an area of growth for us.

There is the general movement toward targeted attacks. Back when I first got involved in this game, if you will, back in the 1990s, as a line cyber prosecutor in the Computer Crime and Intellectual Property Section at the Department of Justice (DOJ), hackers mostly were doing things like tearing down Web pages and putting up pictures on the DOJ Web page of a Nazi symbol and those sorts of things that were annoying, but more annoying than anything else. And then we went through the period of worms where mass disruption took place, but perhaps little lasting damage.

That is not the world we are in anymore. Hackers are after information of value and actual money, as today's panel indicates, and they are increasingly targeting attacks for the places where they can get value. And that makes things more risky.

There are other elements of our risk profile that are continuing to go up and over which we have little control. I call them connectivity, complexity, and criticality.

Connectivity: We are increasingly connecting all of our systems in more and more different ways, so everybody has always-on, high-bandwidth connections, and there are increasingly international connections, and we are building up this vast network that makes us all able to do more but, as the Chairman indicated in his opening remarks, also makes us more vulnerable.

Complexity: We are connecting more and more devices, from smart phones to embedded devices; TVs are connected to the Internet now. And as we put all of these different devices together, running many different types of software, the mere complexity of the ecosystem makes it harder and harder to secure.

[1] The prepared statement of Mr. Reitinger appears in the Appendix on page 183.

Last, criticality: We depend on this network of networks and the machines that are connected to it every day, not only to play, to do things like social networking, but for the basic functions of our government and economy. And that imposes upon us a need not to stand still.

I do believe over the last 10 years we have made progress, but we have not made enough. We have to make more. And as the Cyberspace Policy Review indicated, the status quo is simply not sufficient. We all need to work together in even stronger partnership to address the growing threats that we face and, to echo another of the Chairman's comments, to do so at Internet speed, not just in law enforcement, although working at Internet speed in law enforcement is a significant problem.

When I was at the Computer Crime and Intellectual Property Section, one of the things we did was work on negotiating the Council of Europe Cyber Crime Convention. That was a first step, but we need to go further to build the law enforcement and specifically the operational relationships that are international and will allow us to respond effectively.

I would like to highlight a couple of the things that we are doing specifically around partnerships within DHS to address this.

First, it is critically important that we continue to build partnership across government. This is another area where I think we have been effective but can grow more effective. I well remember the very first hacker case that I did when I first joined the Computer Crime Section back in the 1990s. I was a DOJ prosecutor, and it was investigated by the Secret Service. So that was then a Department of Treasury-Department of Justice collaboration. We started there. We have continued to grow, and we are in a place now where people have come into positions across the Federal Government. I think we have put a strong team together not only in DHS but in multiple government agencies so that we can work very effectively together.

In DHS, we are working very hard to continue to up our game and build our capabilities. I am perhaps most focused on the people part of this because I am a big believer that organizations fail or succeed based on the people that they have. I have some great people and an awesome team, but I do not have enough of them. I am in the process of trying to grow the National Cyber Security Division. It now has about 111 people on board as of last week, and we want to grow it to 260 people next year. So that is a heavy lift in government, but we are committed to doing our best to fulfill it.

We also need to continue to work better and faster and more effectively with the private sector. I have seen this from both sides. I started in the Department of Justice. I worked for the Department of Defense. I spent about 6 years in the private sector where I had the honor of being the President of the Information Technology Information Sharing and Analysis Center (IT–ISAC), a companion organization to the FS–ISAC, before I joined DHS again earlier this year. And I have seen incredible commitment from people in both the private sector and public sector. I believe we have a real opportunity here. And we have built partnerships, but there is a lot more to do.

In particular, we have built the ways to work together. We have built the framework to work together. Now we need to drive toward outcomes. We need to worry less about having a partnership and more about what we can achieve with the partnership. So let me highlight a few quick examples of some of the things that I think we need to focus on for the coming few months.

The first is the National Cyber Incident Response Plan. This was called for in the President's Cyberspace Policy Review. It may sound kind of highfalutin' and sort of meta, but it is actually not. The idea is that we need, if something bad happens, a mechanism, a very actionable way for all of the relevant government agencies and all of the different entities across the private sector to come together as one Nation—not one government, not one sector, but one Nation to respond to the incident. And we kicked off that process as called for in the Cyberspace Policy Review. It is a broad process, and we are doing this differently than is the traditional government process.

The traditional process is you get together, you talk and talk and talk, and when it is 99 percent done, you go to the private sector, and you say, "What do you think about it?" Or maybe when it is 100 percent done, you ask them for comments. We are not doing that. We have invited the private sector to the table at the very start so that they can help build the foundations of that plan.

Associated with it is the second thing. The private sector has recommended to us for some time that we need to integrate our cyber and communications watch capabilities so we can work together effectively. We are doing that. We are moving towards an integrated watch floor that will combine DHS's different cyber watch centers, like the National Coordinating Center (NCC), which is focused on telecommunications; U.S. Computer Emergency Readiness Team (US–CERT), which is focused on IT; and the National Cyber Security Center, which is focused across government, will be collocated at the same site and able to work together effectively across government and with the private sector, growing our relationship with the private sector and with State, local, tribal, and territorial governments, so we have the organizational mechanisms, partnerships, and trusted relationships to let us implement that Cyber Incident Response Plan process and also work together more actively to mitigate incidents before they become full-blown incidents. We are going to test those processes next year as they get developed in the Cyber Storm II exercise currently scheduled for September 2010.

We will also be in the process over the next year of launching a new and more significant national awareness campaign. We know mostly how to protect systems. Technology is not the barrier. What we need is to get the word out there and to raise the awareness, among other things, of end users and some of these small and local businesses, of how they can protect themselves, the simple steps that they can take, and what the threat looks like. So we are committed to doing that.

I am going to drop a quick footnote that the two private sector members of the panel early on noted the importance of authentication. I would emphasize that we need to do that. The President's Cyberspace Policy Review called for the creation of a Cyber Identity Management Strategy. There is little that we could do that would be more effective to help people protect themselves than to implement strong authentication mechanisms that are available for people's use with privacy built in from the very start. That would enable much better self-protection.

In conclusion, I would say that I think we are at a moment in time when we can really make a difference. We have the right focus across government and with the private sector. We have leadership commitment from the President, and certainly from my secretary and deputy secretary, and the right people coming into key positions in the private sector. I think we can make a real difference as a community.

With that, I look forward to your questions. Thank you.

Chairman LIEBERMAN. Thanks very much, Mr. Reitinger. I appreciate both the substance and the spirit of your opening statement.

Let us start with 7-minute rounds for Senator Collins and myself.

I am fascinated by the global nature of cyber crime. I am curious if we know, in this case of Mr. Gonzalez, how did he connect with the Eastern European gangs that he presumably was working with in the cyber crimes? Mr. Merritt, do you have that answer?

Mr. MERRITT. Yes, sir. Let me put it in perspective. We have talked about compromise today and the exfiltration of proprietary information, such as credit and debit card information from financial and banking institutions. Here is where they end up. They end up in what we call "carding portals," or "carding websites." The best description, in the short time we have today, is that the carding portals are to the criminals what Craigslist and eBay are to law-abiding citizens.

On these carding portals, you can find anything you need. People that, in fact, have intruded in these companies and exfiltrated credit and debit card information are posting the information there for sale.

Chairman LIEBERMAN. In other words, it is a Web site, basically.

Mr. MERRITT. It is a Web site. What happens in these loosely held criminal hierarchies is that, through reputation, you have people who, in fact, successfully hack into companies and then sell their wares on these Web sites. They do not know each other personally, Mr. Chairman. They know each other by their nicknames on these Web sites, and they conduct business without knowing who they are. You might have some that are involved in recruiting, some that are selling his or her own services, or specialty services, such as hacking or phishing. That is where they meet each other.

So when you say, do they meet each other in a physical complex of the traditional type crime, no, sir. They are known to each other through these various nicknames on carding portals. In these cases, which are transnational in nature, that is how they are able to effectively communicate via the Internet without actually knowing who they are or even where they reside.

Chairman LIEBERMAN. That is really astounding, but also absolutely predictable when you think about it. I will leave it to you how much you want to say since we know they are meeting in these portals for criminal purposes—law enforcement attempts to find its way into those portals, just as if you knew that organized crime figures were meeting at a particular restaurant regularly, or using a particular pay phone, you would find a way to tap that phone or be present in that restaurant.

Mr. MERRITT. I would like to comment at some point in time about what Mr. Nelson said about the involvement of foreign law enforcement because it is an integral component of our success in being able to investigate these types of cases. I will give you a good example of a success story that we had in 2005 about one such carding portal. It was called ShadowCrew.com. It had over 4,400 members. And what we were able to do——

Chairman LIEBERMAN. Let me just stop you a minute. Do you have to pay a fee or have a password to get into the portal?

Mr. MERRITT. You have to have your standing in the criminal community authenticated by other criminals. You cannot just log on. They have to verify that either you have successfully hacked into a company and you have an authorized access code to buy or sell. But, just like in the old criminal scheme that you mentioned at a restaurant, somebody has to vouch for your authenticity as far as being part of the criminal world. We, in here, could not access—and I hope no one here is going to try. We would not access these Web sites since they are only for criminals who are known to each other.

However, in 2005, we successfully conducted an online undercover operation for about 2 years, and were the first Federal law enforcement agency in the United States to actually initiate a Title III on a network. We gained control of this network.

Chairman LIEBERMAN. Just define a Title III for a moment.

Mr. MERRITT. Yes, sir. A Title III, in other words—without the criminals knowing—we were eavesdropping, for lack of a better word, on this criminal server, collecting criminal intelligence, and trying to identify the main players on this particular Web site.

We were fortunate. We affected 28 arrests, with six of those arrests being overseas. Essentially, we shut down that Web site, and shut down that server. We learned a lot of lessons: One, just as Mr. Carr mentioned that he encrypts his information, criminals are now encrypting their information, and hard drives, which makes it more difficult for law enforcement to, in fact, obtain that electronic or digital evidence.

They have also come up with a technology, that at the push of a button or even remotely, they are able to destroy the evidence on their hard drives. So I think a grand kudo for the investigation, is that we affected 28 arrests simultaneously because all it would have taken would have been for one criminal member in the organization to send out an e-mail to notify the rest and that digital evidence would have been destroyed. This is a critical component of our ability to investigate and prosecute these types of cases.

There are about 10 or 12 major carding portals in the world now, and we have shown that we do have success. Despite the anonymity that one presumably has on the Internet, we have dispelled that myth. But it is mind-blowing, so to speak, that these carding portals exist.

Chairman LIEBERMAN. Yes, it really is—so mind-blowing that I forgot my next question. [Laughter.]

Mr. MERRITT. Well, you know what? If you do not mind, Mr. Nelson mentioned that one of the challenges we face is the anonymity of these criminals, Mr. Chairman. It is cumbersome and laborious to identify who they are. More often than not, what we experience here in the United States is that many of the intrusions targeting our banking and financial infrastructures, our retailers, and our databases originate overseas. That is where the level of interaction with foreign law enforcement sometimes varies. Different countries have different levels of ability to investigate these types of crimes. Some countries, quite frankly, lack legislation which allows their investigators to prosecute these types of crimes. He mentioned the corruption level. That is true. In different countries, one can have a very loose or, in some cases, direct affiliation between the government and some of these hackers.

Chairman LIEBERMAN. Yes, I was going to ask Mr. Nelson about that. But I am regaining my balance. I remember, and the question was this: Is there evidence the traditional organized crime syndicates, families, whatever, are involved now in cyber crime?

Mr. MERRITT. When you say "traditional," it has been our experience that, unlike the traditional Cosa Nostras that we had years ago, there is organized crime, but it is a loosely held hierarchy because they do not know each other personally.

Chairman LIEBERMAN. And it is a different operation. It is not out of an existing organized crime family here in the United States that had a territory that it controlled for gambling and drug——

Mr. MERRITT. No, sir. You are correct.

Chairman LIEBERMAN. This is new. In a sense, these are new organized cyber crime operations.

Mr. MERRITT. Absolutely. You might have a hacker who is renowned for his or her specialty in the Ukraine. You might have a carder who sits in the Baltics and somebody that organizes these people, who sits in Russia. So it is a loosely held hierarchy within the criminal underworld. But they do not necessarily know each other's identity, if that helps, sir.

Chairman LIEBERMAN. Well, it does, and it obviously complicates the job of law enforcement in trying to find them and break it up.

Mr. MERRITT. Yes, sir.

Chairman LIEBERMAN. My time is up. Senator Collins.

Senator COLLINS. Thank you.

Mr. Carr, in looking at the indictment of the individual who was involved in the computer theft from Heartland, 7-Eleven, and Hannaford, I was astounded at what a long period elapsed where these hackers were able to steal the credit card numbers and debit card numbers. According to the indictment, they operated from between October 2006 to May 2008. That is more than a year and a half.

So explain to me how a breach of that magnitude could go undetected for so long.

Mr. CARR. The way breaches are normally detected is that fraudulent use of cards is determined, and there was no hint of fraudulent use of cards that came to our attention until towards the end of 2008.

Senator COLLINS. But are there no computer programs that one can use to check to see if an intrusion has occurred?

Mr. CARR. There are, but the cyber criminals are very good at masking themselves, and we formed the Payment Processors Information Sharing Council with Mr. Nelson primarily so that the payment processors could share that information. And, in fact, at our May meeting, we did distribute the actual malware that was used at Heartland and we believe other businesses. And at our meeting last week we updated that, and there were three additional malware attacks that had been found since May that one of our constituents had passed out to the membership as well.

So being able to scan systems to know what the malware is, you have to know something about the attack vector, and you have to know something about the malware to find it. All of us in this, we go through annual assessments, but the bad guys are working together to try to get around all those assessments.

Senator COLLINS. But it is my understanding that in this case all of the players met the current standards for cyber security. Is that correct? The voluntary industry-based standards?

Mr. CARR. We passed, we were certified to be compliant with the standards on April 30, 2008.

Senator COLLINS. So what does that tell us about the standards?

Mr. CARR. Well, the standards are good standards. They are necessary. But some of us believe that an enhanced security is possible. A number of years ago, the U.S. Mint decided that it was too easy to counterfeit the old bills and upgraded the technology of the currency. And 30 years ago, when the magnetic stripe was invented, it was invented with the card number in the clear on the stripe. And the systems were all developed to process that magnetic stripe in the clear.

We think it is time for that data to be encrypted so that merchants never have those card numbers in their system and the processors never have that card number in their system either.

Senator COLLINS. Because it would be encrypted from the point of sale to the processor before going to the credit card company?

Mr. CARR. Correct, and throughout the entire system.

Senator COLLINS. Is it typical when a consumer uses a credit card at a retailer that it goes first to an entity like Heartland? I was under the impression that it went directly to Visa or MasterCard or to the bank.

Mr. CARR. Yes, when the card is swiped, it goes either into a gateway that goes to a processor, or it goes directly to the processor, and the banks hire companies like Heartland to be the gateways and the processing entities for the authorizations and the capture and settlement of that information.

Senator COLLINS. So is the problem in this case the lack of encryption between the retailer and the processing entity or the processing entity and the ultimate credit card company?

Mr. CARR. There are actually five—without getting too technical, we think there are five zones of encryption. The first zone is from the moment that card is swiped until it gets into the gateway or into the processing system. And merchants would like to have those card numbers encrypted during that zone because then they would not have that data that could be taken.

Zone two is in the processing network. Zone three is in the computer systems of the processing network. Zone four is data at rest, which is part of the requirements today that all that data be encrypted. And I think the industry has done a good job of implementing that. And then zone five is to the card brands and the issuing institutions as well.

So it is good to have each one of those zones encrypted, but the best is to have them all done, and that is what we are trying to adopt through the various work that we are doing.

Senator COLLINS. Mr. Nelson, when a retailer is the victim of a computer theft scheme like this, do retailers know whom to go to in the government?

Mr. NELSON. I am actually going to defer that to Mr. Carr.

Senator COLLINS. Maybe I will go back to Mr. Carr.

Mr. NELSON. That is more his bailiwick.

Mr. CARR. Do the retailers know what law enforcement to go to?

Senator COLLINS. Yes.

Mr. CARR. I think the larger the merchant is, the more likely it is that they know. But I think we could do a better job of educating all of our merchants about what process they should go through once they are hacked. And, fortunately, Mr. Nelson has agreed to—we have set up a new classification of membership in our organization that will allow members to learn that kind of information.

Mr. NELSON. Yes, I met with the National Retail Federation in June to discuss how we could do more together, and I think there really is not a 24/7 operation in the retail community, which is an important part of this. We need to make sure they are a part of this group and maybe have a link to them, even through our organization.

Senator COLLINS. To whom do they go?

Mr. NELSON. The National Retail Federation has a risk committee, but it is more a 9 to 5 staff that shares some e-mails.

Senator COLLINS. Exactly my point. I mean, Mr. Merritt has told us of the Secret Service's success in carrying off this simultaneous arrest of 20 individuals and the fact that the operation could have been blown with just one e-mail being sent out.

Well, similarly, when a retailer learns that it has been the subject of a computer breach, time is of the essence. I was shocked to learn that in the Hannaford case, which involved other retailers as well, a year and a half went by when these breaches were occurring. So part of the problem here is that once a breach is discovered, I do not think there is an understanding of to whom you go. Do you call the local police? Do you call the Secret Service? Do you call your trade association? Do you call the local district attorney? What do you do? To whom do you go?

Mr. NELSON. We have done a pretty good job in our sector getting the banks to call us, but I think we really need to do a better job reaching out to the retailer community. Again, they are not part of our FS–ISAC. Can we make them part of it? And that is what Mr. Carr has been pushing for, and my Chairman has actually been pushing for that, too. So I think we are going to start looking at that.

Some of the attack signatures that were shared last week, we need to get that out to the retailers, too.

Senator COLLINS. Just the answers here—and I appreciate very much the hard work that all of you on this panel are doing, but the lack of clarity to answer that basic question is troubling to me because if a large retailer is uncertain who to go to, think what it is like for a small business. I think we need far more clarity in answering that question because it is going to be a lot easier for the business community if there is a single source to go to, and also if it is clear who could help you prevent a breach in the first place.

Mr. NELSON. I think Mr. Reitinger's suggestion for a joint operations center where you have private sector and public sector people collocated and that is the source you go to, I think we need to get moving on that.

Mr. REITINGER. If I might, ma'am.

Senator COLLINS. I know I have exceeded my time, and I apologize, Mr. Chairman.

Chairman LIEBERMAN. Go right ahead. No problem.

Senator COLLINS. Mr. Reitinger.

Mr. REITINGER. Thank you, ma'am. There are a lot of resources out there to help businesses to know to whom to report cyber crime. My recollection is both the FBI and the Secret Service list that on their Web pages. We have information on our Web pages on to whom to report, as does the Department of Justice.

I am not so sure that it is bad that there is a diversity of places to report as long as the resources are available to follow up and investigate. There is also the Internet Crime Complaint Center, which is, I think, driven by the FBI.

So there are many resources that can be brought to bear. One of the things that we definitely need to do is do a better job on awareness: Get the word out there and then make sure we have the mechanisms for exchanging data and for law enforcement to work together so the case can be most appropriately addressed and followed up.

Senator COLLINS. Thank you. I still think there is a lack of clarity here. After all, the Federal Trade Commission (FTC) is involved to some extent; the Secret Service is involved; the FBI is involved; the Department of Homeland Security's Infrastructure Protection Division is involved; and State and local law enforcement are involved.

Mr. NELSON. Just to support your argument a little bit more, I think if you go to local law enforcement, sometimes they will not take the case because it does not meet a certain threshold. Let us say it is $100,000. But that particular attack might have been coming from the same entity in some Eastern European country, and they are attacking hundreds of different companies. So, cumulatively, it might be a multi-million-dollar attack. That is the issue.

Senator COLLINS. That is exactly the issue because what may seem to be an isolated attack affecting one business in one State may, in fact, be part of a network of attacks on several different businesses. And we need to have a way to look for those patterns.

Mr. CARR. Senator, I think the stakeholders in the industry would all agree with you. How can that be done?

Senator COLLINS. Right.

Mr. CARR. How can that be communicated and so on? And I think that is a challenge we have to resolve.

Senator COLLINS. Thank you. My apologies.

Chairman LIEBERMAN. Oh, not at all. I appreciate the line of questioning.

Mr. Nelson, in your statement you mentioned the alert sent out by FS–ISAC on August 24 that listed several best practices and recommended controls for companies. I think it is important to note the public-private collaboration that went into issuing that August 24 alert.

As I understand it, it was the first time that the FBI actually brought private sector representatives into their offices and showed you raw intelligence on a threat impacting your sector and asked for your assistance in determining protective recommendations for industry.

I want to follow up on that first by asking you, Mr. Reitinger, this question: Does DHS issue best practices for the various sectors at this point? And if not, do you intend to? If so, are there ways to measure the success of those recommendations, that is, the degree of implementation or follow-up by people receiving those notices?

Mr. REITINGER. I would not say, sir, that it is a set of specific practices that are issued sector by sector. We issue broad guidance from the general how to protect yourself down to the very specific technical alerts that US–CERT regularly produces. So far this year, we have produced over 40 specific products, and our products are available—at least our general products are available on our Web page, including cyber security tips for businesses, how to protect the workplace, those sorts of items.

We also work very closely with the private sector to produce specific incident-related guidance. For example, when the distributed denial-of-service attacks were launched around July 4 of this year, US–CERT worked very closely with our partners in government and industry and produced two distinct products: A Federal information notice that provided information on the attacks and advice on mitigations to the government; and a critical infrastructure information notice that similarly went in a non-public way to key private sector entities throughout the infrastructure, including all of the ISACs.

So, in general, we do produce the products. We also work broadly with the sectors and broadly across the sectors in the cyber security cross-sector working group, which is one way under the National Infrastructure Protection framework that we address cyber security horizontally across all the sectors.

With regard to measuring implementation, as I think both of the Senators' comments indicated early on, metrics are an area of growth, I think, for us, generally. By "us," I mean not just DHS, although I include DHS in that. But in cyber security, judging what works and what does not work is very difficult to do.

So, for example, Senator Collins spoke about the fact that we need to use the procurement power to increase the security of hardware and software that is bought. I could not agree more. But we also need better ways to judge what software is secure so that we can have an effective regime because good metrics drive good behavior and bad metrics drive bad behavior. Similarly, we need better metrics about what security practices work effectively and do not work effectively.

I think our ability in DHS, to return to your question, Senator, to judge how broadly our recommendations are implemented is an area that we need to grow, but have not fully developed yet.

Chairman LIEBERMAN. So that is a priority for you as you go forward.

Mr. REITINGER. Yes, sir.

Chairman LIEBERMAN. In your testimony, Mr. Reitinger, you stated that DHS is building an integrated cyber security and communications watch floor that you expect to be operational before the end of this year, and I think that is a very good development, and I thank you for it and I hope you will push it forward.

I wanted to ask you two things about that, if you could provide, to the extent that you are able, more information about the Department's plans in that regard. But also, building on this line of questioning, do you expect robust private sector participation on the cyber side when this watch floor is completed?

Mr. REITINGER. Yes, sir. The watch floor is in development right now. If you were to travel to our Glebe Road facility, you would see a lot of people doing demolition and building, and I would welcome your presence there. We believe it will open substantially before the end of the year, and the processes for how it will work are under development right now.

With regard to your second question about private sector participation, we already have private sector participation, particularly through the National Coordinating Center, which has a number of telecommunications representatives that are physically present within DHS space and others who are virtually present on a regular basis. We intend to grow from that core broader private sector participation and State and local participation.

Chairman LIEBERMAN. Good.

Mr. REITINGER. Because it is absolutely essential that we be able in certain cases to work together, as I like to say, breathing the same air to build the trusted relationships, and be able to work together virtually so we have a full, one-nation incident response organization.

Chairman LIEBERMAN. That is great to hear. I think one of the most significant recommendations of the 9/11 Commission, which I am proud that our Committee played an active role in implementing, was the creation of the National Counterterrorism Center, and it is really—appropriately, I suppose—one of the unsung heroes of defense of our homeland security. Even in the cyber age, there is something to be said for having people working on the same problem trying to defend the country from the same kinds of threats, breathing the same air, because there is natural interaction that goes on. So I am pleased to hear about that.

Will the watch floor be under the National Cyber Security Division?

Mr. REITINGER. It will be in the spaces of cyber security and communications, but it will include US–CERT, which is part of the National Cyber Security Division (NCSD)——

Chairman LIEBERMAN. Right.

Mr. REITINGER [continuing]. And the National Coordinating Center, which is a part of the National Communications System, but also a part of the Office of Cyber Security and Communications

(CSC), and it will also include the National Cyber Security Center. I am also the Director of that. It is not a part of CSC or the National Protection and Programs Directorate. In my capacity as the Director, I report directly to the Secretary of Homeland Security. The National Cyber Security Center has the mission to coordinate and drive common situational awareness across all of the high-value watch centers for cyber across the Federal Government, and all of those pieces will be collocated.

Chairman LIEBERMAN. That is the key. I mean, as you were describing the acronyms and what they stand for, it began to sound like a very complicated organizational chart. And maybe there is a good reason for every one of those organizations, but the key, as we have found, is to make sure they are all working together and they are not getting stovepiped.

Let me ask a final question along this line going back to the August 24 alert sent out by FS–ISAC. There were some real interesting recommendations in there, I thought, among other things one that recommended that people never access bank, brokerage, or financial services information at Internet cafes or public libraries.

Mr. Nelson, or anyone else on the panel, but we will start with you, is this advice that every American should be following? And if so, why?

Mr. NELSON. Yes, because the information that you key into that computer in a public library or Internet cafe can be kept there. So when you are keying in your user ID and password, a user could subsequently steal it, or they may have put some malware on that computer that you are not aware of, and then they have access to your banking account.

Chairman LIEBERMAN. I hope people are listening. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Reitinger, you brought up the issue of using the Federal Government's procurement power to persuade vendors to deliver safer IT systems, and we had testimony at our April hearing on just this issue from the Director of Research for the SANS Institute. He pointed out that when that is done, the cost of the security software falls dramatically. He cited an example of some encryption software that costs $243 on the retail level, and the Department of Agriculture was able to purchase it for $12, and DOD for less than $6 per copy because of the large volume.

More to the point, however, is this expert's assertion that, despite Federal acquisition rules that requires security to be baked into procurements at the beginning, most times it is not, that there are no penalties or even checks to ensure that security is part of the acquisition process.

What is DHS doing to ensure that security is part of the computer acquisition process?

Mr. REITINGER. Yes, ma'am, I would be glad to talk about that. We have a special software assurance effort that is being driven out of the National Cyber Security Division which includes both a Software Assurance Forum where best practices are developed, industry talks to industry and industry talks to government, work is done around building the business case to help companies understand what they need to do or ought to do for secure development, and work is done on things such as acquisitions.

We also have a Web site called the "Build Security In" Web site that helps to disseminate those best practices more broadly and explain how secure development can be done.

I think in the long term this is an area for growth. It is still too difficult, despite everyone's best work, to know whether software is developed securely or not. So one could say in an acquisition, "Thou shalt only buy securely developed software," but actually specifying that is hard. A lot of work has been done, including recently some private sector groups have developed guidelines for what that might mean, but the evaluation regimes that we have for software remain somewhat rudimentary in terms of their ability to judge that, including the common criteria, which is an international standard which gives a thumbs up or thumbs down for software, which focuses more on the implementation of security features in the software, as opposed to whether the software was developed securely and its overall security.

So there is a lot of work to be done here, both in terms of raising awareness with companies, in terms of figuring out what is securely developed or not securely developed and how to specify that in acquisitions, and then the research and development around how one could develop software more securely which could benefit the entire ecosystem.

Senator COLLINS. And, of course, it never ends because the criminals become more innovative and defeat the security software, which is why it is difficult to mandate specific standards. You have to constantly share best practices, but the technology is going to continually evolve and the criminals are going to continually try to defeat it.

Let me in my final question just ask you about a specific example that was brought to my attention recently by the CEO of a technology company, who was very concerned that there is a lack of a coherent cyber security policy at the Federal Government, particularly in the civilian agencies. DOD is a whole different animal in this case, as is so frequently the case. He cited a recent Request for Proposal (RFP) from the Social Security Administration as an example of his concern about the current inadequacy of the Federal Government related to cyber security.

The Social Security Administration had issued a RFP for a platform that would allow Social Security beneficiaries to access their accounts online and to make adjustments online, such as address changes. He believes that, as drafted, the RFP is highly likely to produce a platform that would make the users vulnerable to spoofing—that is, directing users unknowingly to false Web sites—and that the Social Security Administration would lose millions in just the first month as hackers direct payments elsewhere.

Now, I do not know if this individual's assessment is correct, but it really concerns me that this individual, who is a technology expert, has reviewed this RFP and concluded that the systems to be procured will be highly vulnerable. So what do we do in a situation like this? And how can we get civilian agencies within the government to recognize that they are the container of personal data that, if it is breached, will cause great harm? We have seen example after example—such as the sizeable breach of the Department of Veterans Affairs records a couple years ago.

Mr. REITINGER. So let me answer this in two parts, if I could, ma'am. First, obviously—and I cannot speak to that RFP. I apologize. I have not read it.

Senator COLLINS. Right. I did not expect you to be able to.

Mr. REITINGER. But we do need generally to continue to raise awareness not just with the private sector but with our partners across government, because we are in sort of a generational hump, if you will—we did not all grow up working with computers and understanding computer security, much like we all grew up understanding cars and how to drive cars. So we have to get through this period and make sure that we raise awareness broadly throughout the Federal Government, including among those doing acquisitions.

I do believe we have a Federal Government cyber security strategy. We have the 2003 National Strategy, and then the Comprehensive National Cybersecurity Initiative (CNCI), as recently expanded upon and developed by the Cyberspace Policy Review, which is going to lead to a revised new national strategy. But we have focus and we have a way that we are moving forward.

Specifically around the question that you raise in terms of access to personal data, it is a difficult problem because right now people are accessing whether private or government systems, with a set of computers that they find very difficult to secure, and using a set of methods to authenticate themselves, that are subject to theft.

In the mid- to long-term, we need to move to an environment where no one uses user names and passwords to access sensitive data like personally identifiable information, where one has readily available stronger authentication means, like certificates or tokens or whatever is used, to access data where it is much harder to steal that credential. That will enable great protection in the ecosystem. It will make it harder to steal people's personally identifiable information. And it will make theft of personally identifiable information less valuable because you will not be able to actually take a person's user name and password, or phish it, and then use it against them. You would actually have to take something else.

That is called for in the Cyberspace Policy Review, and it is related to some of the comments that my private sector colleagues made earlier.

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

Chairman LIEBERMAN. Senator Collins, thank you. Just a few more questions.

Mr. Carr, going back to the case that you unfortunately went through, we know that your system was compromised in the sense that, you might say, the front door was knocked down, the cyber criminals got inside the system. There were 130 million accounts that were vulnerable. I presume that a certain number of people involved complained to their credit card companies or the merchants and said, "Hey, I did not buy this, and it is on my bill." Do you have any idea at this point of the scope of the loss, either in dollar terms or how many people were affected? Or is it too soon to say?

Mr. CARR. It is too soon to say. We know that we have charged off on our profit and loss statement $32 million.

Chairman LIEBERMAN. Say that again? I am sorry.

Mr. CARR. $32 million.

Chairman LIEBERMAN. That you charged off?

Mr. CARR. That we have had to expend to deal with this breach.

Chairman LIEBERMAN. In other words, to reimburse people?

Mr. CARR. No—well, part of that could be deemed to be part of that. We do not know the extent of the fraud that was involved at this point. We do not know how many card numbers exactly were compromised.

Chairman LIEBERMAN. Right. What was the $32 million for?

Mr. CARR. That was for forensics work, for legal work, and for potential settlements of some of the claims.

Chairman LIEBERMAN. People complaining about what they take to be unwarranted charges on their cards, would that information come to you? Or is it more likely to come to the credit card company?

Mr. CARR. It comes to the issuing bank and——

Chairman LIEBERMAN. Yes, because most people do not know about you.

Mr. CARR. Correct.

Chairman LIEBERMAN. And then they get back to you, I take it?

Mr. CARR. Right. We are in that process today.

Chairman LIEBERMAN. So at this point, would you say that the number of accounts compromised was small or medium or large? I know you cannot say exactly.

Mr. CARR. It is a significant compromise, but we do not know to what extent.

Chairman LIEBERMAN. In your testimony, you also say that Federal law enforcement was very helpful to Heartland in this process, and I just wanted to ask you to expand on that comment. What kind of assistance did you receive from which agencies?

Mr. CARR. Well, the Secret Service was at our meeting last week and provided some really good information to the members, and we have met with DHS people who have offered to help provide us and our industry some monitoring tools for the security of our computers through some technology that was paid for by the government that is being made available to private industry.

Chairman LIEBERMAN. I appreciate hearing that. As you look back—and I know you have done some work on this and have been spreading the story throughout your business area—what are some of the things you wish you had done, having seen this attack?

Mr. CARR. Well, I wish we had gotten together with our industry and shared information more quickly because by learning how these bad guys attack others, we would have learned a lot at that point. I wish we had done that earlier.

Chairman LIEBERMAN. Mr. Merritt, let me ask you, and then if anyone else wants to get into this, do you think there is a need for amendment of existing criminal laws or adoption of new criminal laws to facilitate the charging or even investigation, but particularly the charging of cyber criminals? Or are you able to operate in this new area within the general parameters of existing criminal law?

Mr. MERRITT. No, sir. In my opinion, we have the necessary statutory authority given to us by Congress to investigate these types of crimes and in my written statement, Title 18 of the U.S. Code, Sections 1028, 1029, 1030——

Chairman LIEBERMAN. Right.

Mr. MERRITT. Those are all sufficient to allow us to carry out our responsibility.

Chairman LIEBERMAN. The other part of my question goes a bit beyond your role in the process, and we should and will be talking to the Department of Justice about this. But just from your experience, is it your sense that once you turn cases over, as it were, to the prosecutors, they have enough within existing criminal law to proceed to prosecute these cases?

Mr. MERRITT. We have been fully supported by U.S. Attorneys across the Nation, sir, and specifically Mr. Reitinger mentioned he was a part of them before the Computer Crimes and Intellectual Property Section (CCIPS). We have been very satisfied. I think they have been, too. I would defer to them to see if they are having some issues as far as their authority to prosecute these types of cases. But we have had very good luck, sir. Thank you.

Chairman LIEBERMAN. Thank you.

Mr. Reitinger, as part of your quite remarkable background in preparation for this job, you have had this prosecutorial experience. What is your sense of whether the criminal laws need updating to meet this challenge or whether they are adequate in their current status?

Mr. REITINGER. With apologies, sir, I have been out of that part of the job since I left the Justice Department and went to the Department of Defense back in 2001. So I would defer to my expert colleagues at the Secret Service and the Department of Justice.

Chairman LIEBERMAN. We will talk to them.

Let me ask you a question that I want you all to think about, and we will be in touch with you as we proceed to legislation. I will start with you, Mr. Reitinger, if you have any thoughts now about what are some of the constructive—if you think there are any—things we can do by way of legislation to help you better do your job or carry out your responsibility with regard to cyber security.

Mr. REITINGER. Sir, I do not have any specific requests to make at this time. Obviously, as I gain my experience in this job, I am learning more about what is required and where the shortfalls, if any, may be. I look forward to continuing to work with you and your staff and the Committee staff on those issues.

Chairman LIEBERMAN. Good. Mr. Merritt, any thoughts there?

Mr. MERRITT. Sir, we are aware of several pending pieces of data privacy legislation that Congress is considering in the different committees, that would encourage private industry, when they have been intruded upon, to report those intrusions. We have been very supportive when committees have asked us for any advice, and we will continue to do so.

Chairman LIEBERMAN. Good. Any legislation or other action by Congress that might facilitate this process we talked about earlier of moving ahead with international cooperation in the investigation and prosecution of cyber crime?

Mr. MERRITT. Mr. Chairman, it is very hard for Congress to implement that type of legislation or law overseas. I think one must rely on personal and professional relationships that we and other law enforcement entities are able to establish with our foreign counterparts.

Chairman LIEBERMAN. Are you working with the State Department—or, Mr. Reitinger, let me ask you—in regard to this? In other words, has the development of international conventions, treaties, or working groups to deal with cyber crime become now an element of our foreign policy?

Mr. REITINGER. Well, sir, I think it has been for some time. The Council of Europe Cyber Crime Convention was groundbreaking when it was first developed as the first major convention dealing specifically with cyber in that sense, and I think all of us were greatly pleased when the Senate chose to ratify it. And that has, I think, enabled a much greater degree in terms of international collaboration.

We are actively involved in the Department of Homeland Security in building relationships with our international partners and are hosting a conference, the Meridian Conference in October of this year, where a number of key players will be coming in, as well as working to develop non-law enforcement operational relationships.

Finally, I would say that the Cyberspace Policy Review specifically talked about the need to build international frameworks, and the National Security Telecommunications Advisory Committee produced a report, I believe last year, on the need for a broader international framework around cyber.

And so I think it is a subject of focus. There is a lot of work that remains to be done under the overall leadership of the Department of State.

Chairman LIEBERMAN. While I have the two of you here, I will say, as I said after Mr. Merritt's testimony, that I am impressed and I did not know about all that the Secret Service was doing in regard to cyber crime. Of course, the Secret Service comes into the Department of Homeland Security with a very strong, unique independent history, but the question I want to ask is whether the Secret Service and the other cyber security divisions are adequately integrated—in other words, whether there is, certainly, sharing of information going on. Mr. Merritt mentioned the Electronic Crimes Task Force and the sharing of information going on with State and local law enforcers. But is it also going on within the building, as it were, or within what will be the building?

Mr. REITINGER. I think the answer is yes, sir. I think we can continue to strengthen the relationships, but there is someone from the Secret Service on the NPPD staff. There is a Secret Service liaison specifically at US–CERT. They have a regular working relationship and an ability to collaborate.

I, specifically, on more than one occasion, when I have received a report from US–CERT, have spoken to them about making sure that we were working both with the Secret Service and the FBI to ensure there was appropriate law enforcement follow-up. And there are collaboration mechanisms that the Secret Service and the Bureau use to work broadly within law enforcement.

So I believe the connections are there, and I think as we move forward and build out the US–CERT capabilities, they are going to continue to be enhanced and be more effective.

Chairman LIEBERMAN. Obviously, that is very important.

Mr. Nelson, any thoughts about additional law, Federal law, that could assist FS–ISAC in the work that you are doing?

Mr. NELSON. We did not really specify in our testimony recommendations in that regard, but we do think that there are some things. We could require support of some funding for, for instance, better education, particularly getting the word out on that you do not open that phish that you get, that type phishing campaign. And one of our members, a small member, a financial institution in southern Virginia, came up with the idea of a logo, an anti-phishing logo almost like the no-smoking logo, or "Don't Pollute, Give a Hoot." Remember those old campaigns? But just kind of get the national mind or kind of the national consciousness around the need not to click on these suspicious e-mails. So I think that is one area that I think we could work on.

Chairman LIEBERMAN. One suggestion that has been made to the Committee for legislation is to require in law or encourage or facilitate the creation of some certification process for the private sector—in other words, either administered by a group like yours in your area of our economy, financial services, and in others; or perhaps with some governmental regulatory board which would set minimum standards that we would require private sector entities to follow to defend themselves—and, in the larger sense, all of us—against cyber attack either for purposes of money or terrorism.

Maybe I should start with you, Mr. Reitinger, and ask you whether you have thought about that and if you have any opinion on it.

Mr. REITINGER. I cannot testify to that in particular, sir. I would have to see the details of the proposal. What I would say is I think it is not true that cyber is completely unregulated. Obviously, there are financial regulations. In the chemical sector, for example, there are elements to chemical cyber security regulation embedded in the current Chemical Facility Anti-Terrorism Standards (CFATS) regime. So there is a mixture of degree of regulation, and sometimes when people talk about the proposal you are talking about, they point to what is called the North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC) model.

Obviously, there is a lot to be explored. I think it is beyond dispute that the status quo is not sufficient. We are committed to working within the model we have right now and enabling our private sector partners to succeed. And in terms of whether additional authority is necessary or appropriate, I think we need to continue to examine that, because it is clear that cyber security is a national security and homeland security issue that needs to be fully addressed.

Chairman LIEBERMAN. Yes, I agree. We have not reached a conclusion on this, but it is very important, I think, for the Committee to consider it because the Federal Government clearly cannot do all this on our own. Too much of our critical infrastructure is owned by the private sector, which, of course, is quite appropriate and positive. What responsibility does the society through the government put on the private sector to take at least the minimal set of actions to protect themselves and the larger society from cyber attack?

So I would welcome a first response, Mr. Nelson, and say to you that we would like to keep in touch, and with you, Mr. Carr, as well. Go right ahead.

Mr. NELSON. The one thing I would say, we have, of course, in the financial services industry, a number of regulators. I hear some of our firms complain that regulators are coming in every week, a different set. FDIC comes in, the Federal Reserve comes in the next week, and then you have the Office of the Comptroller of the Currency (OCC), etc.

Chairman LIEBERMAN. Tell them to get ready for the National Cyber Security—— [Laughter.]

Mr. NELSON. I will do that. But I think on the other side, we do have a number of cyber security areas that the examiners are looking at that they are examining on today. One was, a couple years ago, the implementation of a guidance, and a guidance sounds like a loose term, but it was actually a requirement for financial institutions to look at all of their applications to see if multi-factor authentication should be applied, and you have to do that evaluation. Most of the financial institutions, at least for business accounts, do require multi-factor authentication, for instance. Even on the consumer side, there is knowledge-based authentication, for instance, knowing that if I am on my computer, this is the correct IP address for who I normally do business with. So those types of authentication and multi-factor authentication tools are more or less looked at by the examiners today to see if the banks are complying with that.

Could they be stronger? And some of the things that Mr. Carr recommended about strong encryption, that we have recommend, and actually the whole panel has recommended, I think that is something at which we ought to look. But, again, we have stayed away from being too prescriptive with that and wanted to really look at, as technologies change and as the attacking vectors change, how do we respond to that. And I think we really try to make that part of our regulatory regimen today.

Chairman LIEBERMAN. Mr. Carr, do you want to respond at all to that?

Mr. CARR. I would just like to say that at our meeting last week, there was a frustration expressed by law enforcement that they would know some of these bad guys and these criminal rings and go to countries to arrest them, and they were not able to arrest them because of non-cooperation with that country. That would be helpful. I am not sure that legislation can solve that problem, but that is a problem that needs to be solved.

Chairman LIEBERMAN. Yes, but that is the kind of problem that can be solved either at a diplomatic level, through the State Department, or perhaps through the development of more and more international cooperative law enforcement efforts.

Well, that is a topic we are going to consider as we go on to develop the legislation, whether we want to create kind of a good certification seal if you will, whether as some have suggested we go beyond and actually require, for instance, encryption or some other steps to be taken. Those are big steps to take, and we are not going to take them lightly or without adequate consideration.

I want to thank the four of you. It has been a very productive hearing from our point of view, both from the real-life experiences—the nightmarish experience that you have had to go through, Mr. Carr, and, Mr. Nelson, the work that your group is doing—and then, Mr. Merritt and Mr. Reitinger, thanks for what you are doing in response. This is a problem that is not going to go away. It is going to get worse unless we can work together to diminish the threat, which this Committee wants to do everything it can to make it possible by those of you who are out in the field every day.

So we are going to hold the record of this hearing open for 15 days for additional statements or questions. I thank you again for your testimony. The hearing is adjourned.

[Whereupon, at 12:04 p.m., the Committee was adjourned.]

APPENDIX

Prepared Statement of Senator Joseph Lieberman

Cyber Security: Developing a National Strategy

Committee on Homeland Security and Governmental Affairs
April 28, 2009

Good morning and welcome to our hearing on developing a national strategy for cyber security. We've called today's hearing to ask some basic questions: how prepared is our government to prevent and respond to the very serious threat of cyber attacks against America and how can we help the Department of Homeland Security perform this critical mission?

After the September 11th terrorist attacks and the creation of the Department of Homeland Security, safeguarding our information networks became a top priority. Congress gave DHS responsibility to assess and track cyber vulnerabilities, but that responsibility has not been carried out as well as any of us had hoped.

The Obama Administration – – has now completed an urgent 60-day review of cyber policy and structures and we await public release of the review with the expectation it will greatly inform a national strategy to ensure that all agencies and departments, in concert with our private sector partners, are working to raise our cyber guard.

I wish we were farther down the road toward clarity of purpose and unity of effort in this endeavor because it is clear our cyber infrastructure is now under constant attack. Our enemies – whether they are individual hackers, foreign governments, business competitors, organized criminal groups, or terrorists – are one step ahead of our efforts to deter them. That gap must be closed.

From 2003's SQL Slammer to the most recent Conficker worm, thousands of worms, viruses, and so-called "malware" have infected and disabled computers around the world and put sensitive data at risk of loss, theft, or improper disclosure. Privacy breaches are a regular occurrence with identity thefts, stolen credit card numbers, or exposure of financial information. Within the federal government, millions of dollars worth of equipment has been lost and the personal information of millions of veterans compromised. Melissa Hathaway, acting senior Director for Cyberspace for the National and Homeland Security Councils, in a speech last week told of an incident in which 130 automatic teller machines in 49 cities around the world were illicitly emptied over a 30 minute period.

The Wall Street Journal reported last week that the operational information for the Joint Strike Fighter – an advanced stealth-capable warplane – was breached, making it easier for our enemies to defend themselves against it. When 50 million people in eight northeast states and Canada lost power in August 2003, we got a pretty good idea of the fallout that could result from a cyber attack on the electric grid – although I hasten to add that incident was not an intentional attack but caused by broken tree limbs. Recently, we <u>have</u> learned of severe vulnerabilities in our electrical grid and we have read reports that foreign governments seeking to map our infrastructures have intruded into our electric systems on a grand scale.

To address these vulnerabilities, I will be introducing legislation later this week with House Homeland Security Committee Chairman Bennie Thompson.

We know our cyber infrastructure is insecure and our security capabilities are inadequate. The Government Accountability Office and various Inspectors General have been reporting on these weaknesses for years. Last December, the Center for Strategic and International Studies issued a report, listing the vulnerability of cyber networks as one of our major national security threats.

Toward the end of the last Administration, serious thought was being given to securing government networks in a coordinated fashion. The Comprehensive National Cyber Security Initiative (CNCI) was established last year as part of a multi-agency, multi-year plan to secure cyber networks. DHS has taken the lead on portions of the initiative through the National Cyber Security Division, which works with public, private, and international partners to secure our federal cyber assets. I am pleased that the Obama Administration's FY10 budget asks for an increase of funds to bring the National Cyber Security Division (NCSD) budget up to $355 million. But this money must be spent wisely.

DHS also must do more to engage and include the private sector, which owns at least 80 percent of the nation's critical infrastructure, including our energy supply lines, our water systems, the nation's communications and financial networks – essentially the computerized systems that support so much of our way of life. Given its far flung ownership and expertise, private industry must be brought to the table by DHS as we set our national cyber security priorities and improve our national cyber security defenses.

We are fortunate to have with us today some of the leading thinkers in this area who have developed excellent ideas about how to safeguard our cyber infrastructure. Stewart Baker is Former Department of Homeland Security Assistant Secretary for Policy; James Lewis is Director and Senior Fellow for the Technology and Public Policy Program at the Center for Strategic and International Studies, which issued the report I referenced earlier; Alan Paller is Director of Research at the SANS Institute; and Tom Kellermann is Vice President of Security Awareness at Core Security Technologies. Gentlemen, thank you for your attention to the subject. I look forward to our discussion.

Prepared Statement of Senator Susan M. Collins

'Cybersecurity: Developing a National Strategy'

Committee on Homeland Security and Governmental Affairs

April 28, 2009

The information and communications networks we refer to as cyberspace have become critical to our economy, national defense, and homeland security. Yet every week, we learn of more threats to our cyber infrastructure. The specter of our adversaries disrupting our telecommunication system, shutting down our electrical power, or freezing our financial markets is not science fiction. It is a very real possibility as thousands of attacks occur every day. For example:

- Intelligence officials have stated that China and Russia have attempted to map the United States' electrical grid and have left behind software that could be activated later, perhaps to disrupt or destroy components;
- The *Washington Post* has reported that hackers broke into the Pentagon's Joint Strike Fighter project and stole information; and
- Last year, cyber thieves secretly implanted circuitry into keypads sold to British supermarkets, which were then used to steal account information and PIN numbers.

As these intrusions demonstrate, the cybersecurity threat is real, dangerous, and accelerating. Today this Committee will examine the practical issues of how we should organize the federal government to respond effectively. An effective response to cyber threats will require coordination among law enforcement, intelligence agencies, and the private owners of critical infrastructure. The Department of Homeland Security is the crucial nexus of these realms.

Bringing together these three worlds is precisely the reason Congress created DHS following the terrorist attacks of 9/11. The Comprehensive National Cybersecurity Initiative, started last January, recognized the value of the Department's unique perspective by placing the National Cyber Security Center at DHS and charging DHS with responsibility for advancing coordination and consultation among the many federal entities with cybersecurity missions.

Last year, Senator Lieberman and I included cybersecurity provisions in the Homeland Security authorization bill that would have increased the responsibilities of the National Cyber Security Center in DHS.

We need to determine what authorities are necessary for DHS to undertake the mission of better securing federal networks and our nation's critical cyber infrastructure – authorities that must be exercised as the Department works with, but does not supplant, the important roles played by the Department of Defense, the Intelligence Community, federal law enforcement officials, and other agencies.

These authorities must allow the federal government to address some of the most pressing cybersecurity issues, including:

- Sharing critical information on threats and vulnerabilities with the private sector since 85% of critical infrastructure is privately owned;

- Encouraging the adoption of best practices and standards across the government and throughout our nation's critical infrastructure;

- Generating a strategy that deters terrorists and hostile nation-states from executing cyber attacks that could potentially devastate our critical infrastructure;

- Securing the supply chain to ensure that the systems we purchase are free from malicious code; and

- Establishing standards and performance metrics that can guide government procurement and so encourage manufacturers to incorporate better security into their products for the benefit of both the government and the public at large.

Finally, as we consider the organization of our cybersecurity activities, I would note this new Administration has shown a tendency to appoint special assistants and czars within the White House for virtually every problem that comes along. While I understand the need to shine a spotlight on these problems, the creation of numerous czars or special assistants usually leads to conflict, turf battles, and confusing lines of authority.

Moreover, Congress's ability to effectively oversee activities directed from the Executive Office of the President is severely limited. Typically, we cannot call on those in the White House to testify before us, and their budget requests have limited detail. On an issue as pressing and complex as cybersecurity, congressional oversight is crucial to making real progress.

I hope to explore these issues with the witnesses today so that we can provide the basis for legislation to provide DHS with the authorities it needs to secure our nation's information technology systems. As the recent intrusions attest, this issue requires our attention.

STATEMENT

OF

STEWART A. BAKER
PARTNER
STEPTOE & JOHNSON LLP

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

HEARING ENTITLED

"CYBER SECURITY: DEVELOPING A NATIONAL STRATEGY"

PRESENTED ON

APRIL 28, 2009

Chairman Lieberman, Ranking Member Collins, and members of the Committee, I want to begin by thanking the Committee for holding this timely hearing. As a nation, we have never depended more on information technology (IT) networks. Standardized IT networking is often credited with a productivity renaissance, and it has changed the everyday lives of Americans in profound ways. In fifteen years, decentralized networks have moved from novelty uses like monitoring communal coffee machines to managing financial assets, telecommunications, and the electric grid.

That's both good news and bad, because this revolutionary new technology poses real risks. We trust far more of our critical assets to IT networks than we once did, and security vulnerabilities that may have been tolerable fifteen years ago can have devastating consequences today.

Let me give you just one example of the new risks that all this connectivity has introduced into our lives. It's the story of a man named Howard Crank; I heard it from his stepdaughter. Earlier this year, in January, Howard Crank was living quietly at home when he learned that he had won a prize in a Spanish lottery. He needed the money. He was 73 years old, a retired Air Force veteran living on a pension in a modest California duplex. Diabetes had forced the amputation above the knee of both his legs. His wife's health was not good. But he could afford a computer, and it opened new worlds to him. Even a housebound vet could travel the world on the Internet.

The Internet, it appears, is how he discovered that he'd won the lottery. Of course, it turned out that there were transfer taxes to pay before the winnings could be sent to him. It was expensive, but his share of the lottery was also growing – at one point his winnings reached $115 million.

Howard Crank started sending money to clear the taxes and release the funds. His life savings were $90 thousand. He sent that.

It wasn't enough, so he took out a loan secured by his home and sent that. A few weeks later, he took out a second loan on the house and sent that. He maxed out two credit cards and sent that. Perhaps $300 thousand went to Spain. Still not enough. He asked his stepdaughter for $40 thousand.

She thought that was odd. And when he was hospitalized a few weeks later with a broken femur in what remained of his left leg, she checked his financial records. She found that Howard Crank had ruined himself and his wife in response to an apparent Internet hustle. The Spanish scam artists disappeared without a trace. Crank died of a heart attack before he could provide details.

"I think he probably knew it was a fraud at the end. But he was hoping against hope. He'd sent them so much money already, and they were so convincing," his stepdaughter says. "By the end he'd lost his zest for life. He was desperate."

His 79-year-old widow will lose her home and is likely to be forced into bankruptcy by the remaining debts.

Now I don't tell that story because Howard Crank was the victim of some clever security breach. I tell it because the source of the problem was how close the fraudsters could get to him. He would never have let a con man into the quiet life he and his wife were living. But the Internet brought con men from all over the world to his duplex. Just as it bring thieves and spies and soldiers from all over the world to our banks and government offices.

And for one reason more. Howard Crank got real pleasure and value from using the Internet. He could find previously obscure nuggets of information, perhaps the whereabouts of old Vietnam War friends he'd lost touch with, or new charities he could to add to the three dozen he already supported. But in the end, all that connectivity took far more from him, all at once, than it had given in years earlier. So too for us. We may be too cynical to fall for a Spanish lottery email. But more sophisticated attackers will find better ways to get close to us, to know our families, and our finances, and our weaknesses. And if we don't find a way to shore up our defenses and above all to bring accountability to the Internet, more and more Americans will lose everything to organized crime.

And crime is just the most obvious risk. When nation states bring their resources to bear on the exploitation of network vulnerabilities, the danger is even greater. When I was General Counsel of the National Security Agency in the early 1990s, network attacks were rare and difficult. When I came to the Department of Homeland Security in 2005, network attacks were commonplace and highly successful. It's as though the typical score in a soccer game had gone from 1-0 in the 1990s to something like 247-189 today.

The CSIS Commission on Cybersecurity for the 44th Presidency deserves great credit for thoughtfully addressing the crisis that we face. I participated in some of the Commission's proceedings, and I join in many of the recommendations that Commission made. But not all of them. Today, I would like to address two topics, one where I disagree with the Commission and one where I tend to agree. The first, where I disagree, concerns organization. The second, where I agree, touches on the relationship between the federal government and the private sector.

I. The principal organizational recommendation made by the Commission concerns the role of the White House. The Commission recommends that responsibility for cybersecurity be lodged with a new Assistant to the President. This assistant would be supported in the first instance by a National Security Council directorate. As further support, the Commission recommends creating a National Office for Cyberspace, or NOC, in the Executive Office of the President. This office would absorb some of the cybersecurity responsibilities now assigned to DHS, most notably the National Cyber Security Center, or NCSC. Below these offices, DHS and other agencies would continue to exercise their existing authorities, but with new vigor and coordination arising from the clout of the Assistant to the President, the NSC, and the new NOC.

Without intending it, I've become something of an expert in the process of creating new government organizations, having worked to establish two of the three most recent Cabinet departments. I helped Shirley Hustedler start the Education Department in the late 1970s, and at DHS, I started the DHS Office of Policy. That was a startup within a startup. The more I've seen of government reorganizations, the more skeptical I've become about their value, and I'm especially skeptical about the recommendation to create a NOC.

Let me explain why. There is a kind of lifecycle to proposals for new governmental organizations. In the first stage, proposals for organizational change begin to gain momentum -- almost always because the existing organization of government is flawed. After all, no one suggests changes when things are going well. Sometimes there's been a shocking failure, such as the 9/11 attacks that led to the creation of DHS. Sometimes the flaw is a lack of governmental focus on a mission that seems more important than before, as with the Education Department. But we always begin with an existing organization whose flaws have suddenly become especially prominent.

The second stage, when proposals for organizational change become concrete, requires an exercise of imagination. The new organization has to be envisioned. Since the whole point of the new organization is to cure the failings of the old organization, I think it's fair to say that the proponents of change never imagine an understaffed, overworked agency that drops balls. No. More or less by definition, an organization that does not exist does not have any flaws. So there's a great temptation to give this new organization great responsibility. After all, the old agencies have sometimes failed, and the new agency has not.

Unfortunately, that's only the second stage. In the third stage, the new organization actually begins work. In the glare of publicity it takes up its new responsibilities. But as a brand-new agency, it has to hire staff, find space, let contracts, arrange for IT support, and lease copiers, all before it can begin to carry out the missions that it has been assigned. Meanwhile, the agencies that lost ground in the reorganization snipe from the sidelines or make a bid to recapture their old turf. Six months after it's been created, the new agency is still struggling to put in place the basic capabilities that any agency needs to function. Instead of the ideal organization imagined by lawmakers and commission members, the new agency is all too flawed. Only after years of effort does the reorganization begin to produce improvements that the outside world can see.

I've lived that cycle. I've helped write reports that called for the creation of new organizations to respond to existing agencies' flaws. I've joined new organizations full of enthusiasm for the newly imagined perfection that they will embody. And I've labored to deliver perfection in offices that had no light bulbs, no staff, and no way to move paper around the office.

It's that experience that makes me dubious about creating a National Office for Cyberspace. I know that some in Congress find that proposal appealing. The Cybersecurity Act of 2009, recently introduced in the Senate, would create a new office within the Executive Office of the President (EOP) to manage cybersecurity. I also understand the Commission's frustration with DHS. Many of its members dealt with DHS's cybersecurity organization when it was deep in Stage Three of the cycle I have described. In discussing why cybersecurity should be managed from the White House rather than DHS, the Commission says as much. "Managing a complex international effort involving several large and powerful departments would be difficult for any agency, much less one that is still in thè process of organizing itself. Although, [DHS's] performance has improved in recent years, our view is that any improvement to the nation's cybersecurity must go outside of DHS to be effective."

Here, I believe that the commission, and others who wish to strip DHS of cybersecurity responsibilities, fall prey to the perfection of imagined alternatives. But the problems that DHS has faced in organizing itself are likely to be repeated in any new agency created as a substitute for DHS. If the commission is concerned about the difficulty of an agency's improving cybersecurity while also organizing itself, then it should be a bit more cautious about handing that task over to an agency that has not even begun to organize itself.

Compared to the perfection of an imaginary NOC, of course, DHS's flaws look serious. But the NOC will have flaws too. It will have to begin by doing what every new agency has to do – hire staff, build processes, find furniture, and let contracts while at the same time trying to carry out a mission that everyone agrees is urgent. DHS has spent the past year doing exactly that, both for the NCSC and for the Einstein deployments and other operational tasks assigned to it by the last Administration. If DHS has only begun to build that capability after a year, what makes us think that the NOC can organize itself more quickly?

The best argument for putting a large office with quasi-operational responsibilities in the Executive Office of the President is to give it clout, or at least visibility. But clout is a matter of Presidential will, not boxology. The Office of National Drug Control Policy has been in the Executive Office of the President since 1988, but it's fair to say that its clout has varied substantially over the years. By the same token, no one thinks that the Defense or Justice Departments need to be in the White House to demonstrate how seriously every President takes them.

And the price of that imagined clout is high. For the President, of course, putting the NOC in the Executive Office of the President means that responsibility for its success or failure will fall squarely on his shoulders. If the new office turns out as well as we imagine, that may work out fine. But if not, it is the President's managerial decisions that will be criticized. What's more, finding staff and funding and space for a new White House office will be a challenge. Finally, the battle rhythm of any part of the Executive Office of the President leaves little room for long-term work like drafting regulations, setting standards, or overseeing cybersecurity centers. Inevitably, staff will be pulled into the urgent crises that arise every day at the top of their organization. Important projects that can be postponed in the face of emergencies will be postponed, again and again.

In short, I urge the committee, and the Administration, to be cautious about pinning its hopes to a NOC that has no flaws because it doesn't exist. If we start over again, we're likely to be disappointed again. DHS's execution of its responsibilities has certainly not been perfect, but it has spent much of the last year improving on its record. It has able new leadership and a head start on creating the capabilities it needs. I would be inclined to build on that foundation rather than starting over.

For the same reasons, I would be cautious about restructuring all of the advisory committees and information sharing arrangements that DHS administers. First, although I share many of the frustrations that the Commission expressed with the current structure, I question whether the structure of federal advisory committees will make much difference in our long-term preparedness for network attacks. Many of the problems identified by the Commission – a proliferation of Washington representatives and a decline in CEO participation, for example – can be solved without throwing out the current structure. If the President meets regularly with the NSTAC and makes it clear that he expects to be meeting with CEOs, then CEOs will soon fill the NSTAC's ranks, no matter where it is housed.

II. Now let me turn to the relationship between government and the private sector on network security. There is no doubt that it needs to evolve further. The Commission is correct when it says that industry will need help and guidance, perhaps even regulation, to meet this threat. Left to its own devices, the private sector will only invest in network security until marginal costs equal marginal benefits. Put another way, no rational company will spend a dollar on network security to prevent ninety-nine cents worth of loss. Private sector security is inevitably focused on quantifiable, predictable losses, such as theft of services. But not every intruder is a thief or a fraudster. Some of them are spies and saboteurs planning a new form of warfare. Protecting civilians from warfare is not usually a task we leave to the private sector.

Recognizing the need for a government role is the easy part. What's more difficult is developing the expertise that's needed to guide the private sector. Generally speaking, the federal agencies on the civilian side of government are not as sophisticated about network defense as many private sector industries, such as banking. There is reason to believe that improvements in federal capability are likely. DHS is going to increase its own expertise substantially as it oversees the upgrading of federal civilian cybersecurity. That's an essential step if the government is to provide useful guidance to the private sector.

Even more difficult is the task of knowing how to guide the private sector. I do not want to pretend that I have all the answers here. But I think some points are plain. First, this is not an area where laws or even regulations can move as quickly as the threat. A few years ago, it was possible to imagine that improved operating system security would solve most of the problems we faced. If we had written rules then, they would have focused heavily on patches, and updates, and the responsibilities of operating system producers. But Microsoft in particular has devoted enormous resources to building security into its operating system – to making sure that programs cannot run without the user's permission.

And the result is not better security, just better malware. Hackers now often seek out flaws in applications or websites, or they try to fool users into granting permission by clicking on a file that purports to be something it is not. If we find ways to close off this avenue of attack, I fear that new avenues will be opened, and new countermeasures will be necessary. Thus, a system in which the government imposes rigid standards on the private sector through the regulatory process seems doomed to lag behind the threats it seeks to thwart. I would urge great caution before we launch legislative and regulatory efforts to prescribe particular security measures.

Some regulatory regimes try to deal with this problem by imposing procedural rather than substantive requirements on companies -- that is, they require companies to develop and implement their own standards rather than imposing static, one-size-fits-all standards through the regulatory process. For example, the Gramm Leach Bliley Act (GBL Act) seeks to safeguard personal information held by financial institutions by requiring each institution to develop and implement its own security plan. The GLB Act sets out broad objectives for these security plans rather than requiring individual plans to contain certain specific elements. The Federal Energy Regulatory Commission (FERC) appears to be taking a similar approach with respect to cybersecurity. FERC has recently approved critical infrastructure protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cybersecurity breaches. These standards require owners and operators of the bulk power system to establish policies and procedures to safeguard physical and electronic access to control systems and to be prepared to recover from a cyber incident. These standards identify the assets that need to be protected and broadly outline the measures necessary to protect them. The standards, however, impose very few specific security requirements.

This approach has the advantage of flexibility. Assessing a company's current security status and being ready to respond to threats are not requirements that will go out of style. But such procedural approaches run the risk of becoming meaningless. While it might well be useful to apply these flexible standards more broadly, the government is likely to have to find a way to provide guidance, and quite possibly binding guidance, in a way that is far speedier than our current clotted regulatory process allows.

In short, it is clear that the federal government will need to exercise more authority over the private sector to improve network security. But the usual tools – such legislation, regulation, and standards – are not sufficiently flexible or fast-moving to address the problem. Without pretending to have a complete alternative in hand, I think that the most appealing approach will combine procedural requirements, as in Gramm-Leach-Bliley, with fast-moving situationally-driven guidance from a DHS that has, and can draw on, the best security thinking in the federal government.

I thank the Committee for the opportunity to share my thoughts on this topic, and I look forward to working with you and the Department.

Testimony
Senate Committee on Homeland Security and Government Affairs
"Cybersecurity: Developing a National Strategy"
James A. Lewis
Center for Strategic and International Studies
April 28, 2009

I thank the committee for the opportunity to testify. Among the many difficult challenges America faces this year, cybersecurity deserves special attention. If America continues to fail in securing cyberspace, our most important national economic and security interests will suffer critical damage. We must organize and equip ourselves for conflict in cyberspace. Major agencies have key roles to play in this, but their efforts must be coordinated and comprehensive to be effective.

Conflict in cyberspace is best seen as a steady erosion of America's technological, military and economic leadership. This erosion is accompanied by the almost certain risk that our opponents will use cyber attacks against critical infrastructure in the event of a conflict with the United States, but the central problem before us involves espionage and crime. These problems – espionage, crime and risk to critical infrastructure – will never go away, but they can be better managed and the degree of risk can be reduced by coordinated government action.

A brief summary of the current state of our efforts to protect cyber networks is that they are inadequate. This is not a criticism – many people have worked hard in recent years to improve cybersecurity, but we are starting late and we have not done enough. Our opponents are the intelligence and military services of hostile nations and a network of shadowy but highly skilled cybercriminals. They are resourceful, inventive and experienced, and have successfully exploited network vulnerabilities in the United States

The topic of this hearing – developing a national strategy – is very timely. The United States needs a truly comprehensive national strategy that addresses all dimensions of the cybersecurity problem and engages all stakeholders. There is a national strategy, the 2003 National Strategy to Secure Cyberspace, but it is generally perceived as inadequate in part because it relied too heavily on voluntary efforts. There is also the 2008 Comprehensive National Cybersecurity Initiative, but it was not truly comprehensive in that it focused on securing government networks.

In December of 2008, the Center for Strategic and International Studies (CSIS) Cybersecurity Commission laid out a series of recommendations for a comprehensive national approach to cybersecurity. We called for the creation of a strong White House cyber advisor with clear authority over policy and, in coordination with the Office of Management and Budget, over budgets related to cybersecurity. One reason that previous administrations have failed to secure our nation's digital infrastructure is that they have divided responsibility for cybersecurity among many agencies and White House offices. Our opponents exploit these divisions. We proposed creating a new White House office for cyberspace to work with the NSC to manage the many aspects of securing our national networks, consistent with privacy and civil liberties, and to help begin the work of building an "information age" government based on new, more collaborative organizational models.

A comprehensive national strategy for cyberspace would use all the tools of U.S. power in a coordinated fashion – international engagement and diplomacy, military planning and doctrine, economic policy tools and regulation, and the involvement of the intelligence and law enforcement communities. A comprehensive approach should include a public doctrine for cyberspace that makes clear to our foreign partners and adversaries that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the U.S. will protect it, using all instruments of national power.

Our report contained recommendations on many other important elements for improving cybersecurity, including the need for increased education and training, for the modernization of outdated laws, greater use of acquisitions authorities to drive product improvement, and for better authentication of online identity within government and critical infrastructure. A truly national approach must address these issues if it is to succeed.

We also called out the issue of market failure. One of the reasons earlier efforts have not succeeded is that they ignored the disconnect between market forces and national security. We have been waiting for more than a decade for the market to deliver the innovations needed to secure cyberspace. While there has been some improvement, there will never be enough without active White House leadership that is grounded in a clear vision for a secure digital future.

Several of our recommendations may be adopted to some degree by the new administration. As you know, the White House has recently concluded a sixty day review of cybersecurity policy, and while few public details have been released, it is clear from public statements that the White House will play a greater role in organizing cybersecurity policy, that there will be greater attention to international engagement and to relations with the private sector, and closer coordination among agencies. These are all positive developments if they indeed turn out to be the direction that administration policy takes.

My hope would be that the sixty-day review leads to a strong White House cyber advisor with clear authority to set policy and help guide budgets. But there is an intense and unfortunate policy debate within the administration over how much authority the cyber advisor should have and how strenuously the United States should protect its cyber networks. I say unfortunate because our opponents are not waiting sixty days to attack us.

While policy and coordination must be led from the White House, implementation and operational activities should fall upon the agencies. The key agencies for cybersecurity are the National Security Agency and other Intelligence community components, the Department of Homeland Security, the Federal Bureau of Investigation, the Department of Defense and the Departments of State and Commerce. Each of these agencies has a different sphere of responsibility, although there is some overlap, and different expertise.

Operational responsibility for cybersecurity falls primarily upon NSA, FBI and DHS. NSA has the expertise, the experience and the resources to defend cyberspace as part of a larger and comprehensive national strategy. Its efforts currently focus on securing military and intelligence networks for the government. FBI has a national presence, strong legal authorities for dealing with cybercrime and has reorganized itself to give cybersecurity greater prominence in its law enforcement mission.

DHS's role is more complex. In the previous administration, the White House assigned DHS the lead role for cybersecurity, but this was beyond its competencies. DHS is not the agency to lead intelligence, military, diplomatic or law enforcement activities. However, this does not mean that DHS does not have an important role. Properly scoping the role and responsibility of DHS and then providing adequate resources for those responsibilities is an urgent task for this administration.

DHS is responsible for securing critical infrastructure. It is also responsible for securing civilian government networks – the "dot gov" networks. It is beginning to build the capabilities needed to carry out these missions. Building this capability requires sustained investment in facilities, technology and in the DHS cyber workforce. At the moment, these are inadequate to the task and increased allocations for cybersecurity are essential.

Some of the resource challenge for DHS revolves around the acquisition and use of technologies to better secure civilian government networks. The CNCI had a program named "Einstein" to provide this surveillance. A year ago, DHS introduced "Einstein II," an upgraded network surveillance system. Neither Einstein nor Einstein II are adequate to the task, and while DHS plans further upgrades (culminating in "Einstein IV"), the immediate question is whether in the interim, there are ways to take advantage of NSA technologies to perform the "dot gov" surveillance mission that provide adequate safeguards for privacy and civil liberties. This is of course a sensitive topic - NSA has the capabilities, DHS has the responsibilities and authorities, but there are compelling constitutional reasons for restricting NSA's role. That said, and despite the worries about giving NSA too large a role, it would be a serious error for DHS not to find ways to take advantage of NSA's skills and capabilities for defensive missions at a time when our government networks are under serious, sustained and successful attack.

DHS may also want to consider some reorganization to improve its performance in cybersecurity. Perhaps the most immediate of these steps would be to merge USCERT and the National Communications System (NCS) and its components into a single entity within the National Cybersecurity Division. It no longer makes sense to separate cyber and telecom.

DHS's cyber functions are part of its larger National Protection and Programs Directorate. This Directorate faces a strategic challenge in better integrating the plans for physical infrastructure and cyber infrastructure protection and resiliency, and for making these plans more focused and less cumbersome. The 2009 National Infrastructure Protection Plan, although it is 188 pages, could be improved with a more precise definition of critical infrastructure, a better assessment of risks and a greater focus on action. The NIPP is not actually a plan, and DHS might benefit from creating separate, short, and implementable plans on how to protect critical infrastructure, increase resiliency, and assure the delivery of critical services in the face of attack.

As part of its critical infrastructure responsibilities, DHS is the Federal interface with private sector critical infrastructure owners and operators. There is a plethora of partnership groups; none are sufficient. DHS may wish to look at the Department of Defense's "Defense Industrial

Base" (DIB) effort as a form for a new approach to partnership and information sharing. While the DIB does not translate exactly to DHS's responsibilities, it has had some success and DHS should examine it closely as a way to reengineer public-private partnerships.

The overall question of how to improve cybersecurity in critical infrastructure is a difficult one. We know that current levels of protection are very uneven. Changing this raises troubling questions of regulation and investment. The United States has previously relied on voluntary action by critical infrastructure to provide adequate security, but to quote the former chairman of the Security and Exchange Commission, Christopher Cox, a longtime proponent of deregulation, "The last six months have made it abundantly clear that voluntary regulation does not work." A new Federal approach to cybersecurity must elicit actions from the private sector that it would not otherwise perform.

Government intervention in response to market failure can include regulation (or the threat of regulation) or subsidy. Both have limitations, but both are preferable to inaction. Currently, DHS does not have regulatory authority for most critical infrastructure, but rather than giving DHS new and expansive authorities, it might be better to use existing agencies, such as the FCC, FERC, the NRC and others, to guide their respective sectors to better cybersecurity. Cybersecurity must become a priority for regulators. This sort of prioritization and coordination among many different agencies is best done from the White House.

Defensive efforts alone cannot improve cybersecurity. The United States needs to develop a strong offensive capability and place this capability in the context of a well-defined chain of command leading up to the President. An offensive capability can contribute to a cyber-deterrent and help inform out own defensive efforts. The United States must shape the international environment to improve cyberspace, by increasing multilateral cooperation in law enforcement to shrink the sanctuaries for cybercrime that currently exist. We need to expand relationships with our allies for mutual defense in cyberspace and work with the international community to develop norms and sanctions for hostile action in cyberspace – no nation should be able to brag, as Russia has, about its exploits in Estonia and Georgia and not face some consequence. Federal incentives and regulation can help create the innovation we lack in cybersecurity, and federal investment in research that complements private sector efforts can help provide the long-term basis for secure networks.

This is a complex agenda. It will not be easy to achieve. However, the United States is in a very unfortunate situation. We have taken better advantage of cyberspace than our competitors have, and this has provided real economic benefits. Our reliance on cyberspace holds the potential for economic recovery and future growth. However, the combination of greater reliance on cyberspace and inadequate attention to security has left us more vulnerable than our opponents. If we cannot change this, the power and influence of the United States will shrink, and our prosperity and security will be damaged. Congress and the executive branch have the opportunity to avert this damage if we act now.

I thank you for the opportunity to testify and will be happy to take your questions.

Testimony of Alan Paller[1] of the SANS Institute[2]
Before the U. S. Senate Committee on Homeland Security and Government Affairs

Cyber Security: Developing a National Strategy
April 28, 2009

A Brief Summary:

Our nation is facing a wave of increasingly sophisticated cyber attacks that overwhelm the defenses established under the GISRA and FISMA legislation. Congress can reduce the threat of damage from these new cyber attacks both against government and against the critical infrastructure by shifting the government's cyber security emphasis from report writing to automated, real-time defenses implemented through strategic use of the $70 billion of annual federal IT buying power. DHS cannot make that happen; only active White House leadership will get the job done.

Five Findings That May Help Inform Congressional Options in Cyber Security

Part I: Defining the Problem

1. Hackers and nation states have more deeply penetrated civilian government agencies and the critical national infrastructure computer networks than the public and most members of Congress have been told.
2. The attackers are improving their techniques far faster than the US government is improving its defenses. In other words, the threat is increasing at an accelerating rate.

Part II: Promising Options Than Can Turn the Tide Against the Attackers

3. There is strong evidence that federal cyber security can be radically improved through strategic use of federal buying power.
4. Four huge unintended errors make it almost impossible for agencies to make big improvements in IT security. This Committee can fix all four.
5. If you do make these corrections in government, you will, at the same time, be making cyber security much more effective for the critical national infrastructure and the general public.

Part I: Defining the Problem

1. Hackers and nation states have more deeply penetrated civilian government agencies and the critical national infrastructure computer networks than the public and most members of Congress have been told.

Testimony before the House Homeland Security Committee in April 2007 revealed that both State Department and Commerce Department computers had been penetrated, most probably by government-funded actors in China. Although the State Department found the attackers and rooted them out, a Commerce official testified that the department did not know how long the attackers had been controlling department computers nor did they know how far and wide the infections had spread. As a result they had no confidence that the attackers' hold on their systems had been broken. The question of why any nation-states would want to control Commerce Department computers is worth considering. The part of Commerce that was attacked, the BIS division, or the Bureau of Industry and Security, decides which technologies are too sensitive to be exported. Commerce keeps all the data a nation state needs to determine each new technology that matters to us, why it is sensitive, how it works, and who is developing it – giving the attacker a near-perfect roadmap to steal the sensitive technology itself through further attacks on the commercial developers' computers. The defense industrial base is also weak in cyber security, as Time Magazine's 2005 disclosures about the Titan Rain attacks proved, but we'll get back to that later.

State and Commerce attacks were widely reported. What has not been reported is the number of additional sensitive federal agencies that have been just as deeply penetrated by the same attackers. In one department, I was told privately, the damage was so widespread that the department's CIO had to invite the NSA Blue Team experts in to help isolate and eradicate the problem. Additional private communication with cyber security and IT managers in government leads me to conclude that nearly every militarily and economically sensitive element of the government, including the offices of important Congressional Committees, have now been penetrated, sensitive data taken, and in many instances back doors are still open for those attackers to return at will to gather or change information.

One example of this kind of manipulation, and the vulnerability in federal defenses was discovered in a Department of Homeland Security Web site where visitors were redirected to a site set up to take over the visitors' computers. The malicious sited attempted to place keystroke loggers on those unsuspecting citizens' computers and to use the data from the keystroke loggers to steal money from bank accounts or stock trading accounts.

But weaknesses in government cyber defenses are only a third of the problem. A second area that deserves this Committee's attention is the degree to which government contractors and the defense industrial base have also been deeply penetrated, with grave effects.

Government relies on contractors to build and sometimes operate its military and civilian systems. Forbes magazine, Business Week magazine and the Wall Street Journal have revealed that nation states using the same types of advanced attacks used to penetrate government computers successfully attacked computers at key defense contractors. The victims are many of the same contractors that charge hundreds of millions of dollars to tell the government how to secure federal systems.

What has not been reported is that those same contractors have lost some of America's most sensitive new technologies -- and I have been told that those nation states already have put these new technologies to use.

The final important objective, beyond the government, contractors, and the defense industrial base, is protection of the critical national infrastructure, such as the electric grid, the financial system, and the Internet itself. A few weeks ago Americans awoke to learn that the computers that control electric power generation and distribution had been penetrated, most probably by unfriendly nation states. What was not reported was that those same utilities' control systems had been taken over before, by another nation state, and because of the sensitivity of the sources of that information, most utility executives are totally in the dark about those earlier (and probably continuing) infections. We now also know that there are ways to use remote network access to disrupt the power – for days, weeks or even longer. Internet-based attackers have already remotely cut the power in multiple cities outside the US as part of cyber extortion schemes in which they apparently demonstrated their remote control of the power systems in order to collect large amounts of money.

2. The attackers are improving their techniques far faster than the US government is improving its defenses. In other words, the threat is increasing at an accelerating rate.

Three types of highly-motivated and well organized groups are behind this acceleration: nation states looking for strategic information and advantage, organized crime groups looking for profits, and terrorist groups looking for political gain.

China, as just one example, runs a national competition for college and grad school students who may currently be hacking illegally, but who could be effectively employed in creating and using new attack techniques. In 2005, for example, Tan Dailin, a graduate student at Sichuan University who was found hacking into Japanese computers, was recruited for the "Chengdu Military Militia Information Sub-Unit Network Attack and Defense Contest." His team won and, after attending an intensive 16-hour-per-day, 30-day workshop to learn to develop sophisticated attack techniques, his team also won a larger multi-regional competition run by the People's Liberation Army (PLA). The team won 20,000 RMB and set up a company to develop and deploy new attack techniques. By December Tan's signature was found in several hacks into the US DoD. In the summer of 2006, his hacking crew was found to be behind a half-dozen zero-day exploits of Microsoft PowerPoint and Excel used to great effect to penetrate sensitive commercial, military and civilian government sites all over the world and steal tens of thousands of documents. The PLA's competition continues to recruit and develop ever improving talent.

At the same time, organized crime groups in Eastern Europe use money and lies to recruit some of the most sophisticated hackers, and then use terror (credible threats of killing their families) to keep them working even when they decide they do not want to be criminals. These organized crime groups earn hundreds of millions of dollars from cyber crime every year. In one recent case, an organized crime group stole more than $10 million from ATM machines in less than 30 minutes, using stolen data to replicate 45 customers' ATM cards and active control of the bank's computers to increase the withdrawal limits on each of the accounts. The thefts stopped only when the targeted ATMs ran out of cash. With all their money, organized crime groups can afford to pay huge amounts to acquire the best talent and build increasingly powerful new attack tools.

Terrorist organizations also have run hacking schools in Afghanistan and in other countries and use other methods to teach their recruits to hack into computers. On October 12, 2002, Imam Samudra, a senior Al Qaeda operative, planted bombs that killed 202 people including 164 young Australian and New Zealand vacationers on the Indonesian island of Bali. Before he was executed earlier this year, Samudra, known as the "Bali Bomber" wrote his autobiography detailing how others could benefit from hacking. He was a hacker in addition to being a mass murderer. In a chapter in his autobiography called "Hacking, Why Not?" Samudra wrote, "If hacking is successful, get ready to gain windfall income for just 3 to 6 hours working, greater than the income of a policeman of 6 months work. But, please do not do that in the sake of money alone! I want to give motivation to the youth and men who are granted perfect mind by God. I want America and its cronies to be crushed in all aspects." Samudra used hacking to raise money for his cause; we know because one of our graduates in Australia did the forensics on his computer. His chapter on hacking revealed a remarkable understanding of how new recruits can develop the advanced hacking skills needed to break into seemingly sophisticated networks.

The CSIS Commission Report on Cybersecurity for the 44th President has additional examples of the damage that is being done to the nation through cyber attacks and the CSIS proposals for a more effective national strategy are right on target. The remainder of my testimony focuses on two of those proposals that I believe are most in need of this Committee's early action.

Part II: Promising Options Than Can Turn the Tide Against the Attackers

3. There is strong evidence that federal cyber security can be radically improved through strategic use of federal IT buying power.

The most illuminating and encouraging story in federal cyber security is the one that began six years ago when the NSA red team was briefing the CIOs of the Army, Navy, Marines, and Air Force. Red teams test security by attempting to break into networks. NSA's red team was able to penetrate the four military services' systems quickly. The only good news for three of the CIOs was that it took longer to break into their systems than into the fourth CIO's systems.

John Gilligan, CIO of the Air Force at the time, took one of the key NSA executives aside and said, "We will fix every problem you found, but we know you'll come back in a few months and break in just as fast. You are not helping us. Can you get your best attackers together and tell us the most important things we should do, across the Air Force, to make it much harder for you and other attackers to break in?"

NSA agreed and came back saying that when their red teams get in quickly, it is nearly always because of configuration and patching errors. Mr. Gilligan asked if NSA could help the Air Force develop a standard configuration that would block at least 85% of all attacks and still allow Air Force computers to work well. NSA did, with help from DISA and the Air Force and Microsoft. The Air Force has deployed that standard configuration across more than 500,000 computers. In the process, the Air Force saved more than $100 million in procurement costs, that same amount annually in operational costs and tens of millions more in energy costs (because the standard configuration allowed power-saving use without impacting performance.) But even more important is that security patches are now installed in less than 72 hours, instead of the 57 days it took before. And surprisingly, the users are much more content – with help-desk calls reportedly down by 50%.

So here we have a case where security was radically improved, costs were lowered, and the users are happier, as well. Other federal agencies and commercial companies are following in the Air Force's footsteps, deploying that same set of configurations. The federal government's leadership-by-example led Microsoft to make a much more secure configuration template available to many more organizations without charging them any more money.

The Air Force case offers three key lessons:

First, effective defenses can be designed only by people who have comprehensive understanding of how attacks actually work. This is the theme echoed often by Melissa Hathaway of the National Security Council when she says, "Offense must inform defense." Mr. Gilligan has repeatedly said that the Air Force standard configuration project would never have worked were it not for NSA's willingness to translate its understanding of attack techniques into defensive configurations. One of the most common reasons for the federal government's security failures is reliance on the security advice of people who do not know how attacks are executed.

Second, only massive procurement power can persuade vendors to deliver safer systems rather than the standard systems they sell at retail to businesses and consumers. Dozens of customers had asked Microsoft for more secure configurations and all were refused or were asked to pay large amounts of money for consulting services to develop customized settings. The Air Force was about to spend $500 million on Microsoft software over six years. That was enough to get the company to deliver systems with secure configurations baked in, to make it available across all of government, and to build infrastructure to support the Air Force and other users of the secure configurations. When vendors are able to make large sales, they will often lower the costs for each user. This was proven in the GSA/DoD encryption purchase in which software that cost $243 retail and $97 under GSA contract was purchased by the Department of Agriculture, in large volume, for less than $12 and by DoD for less than $6. The vendors still make a great deal of money because the volume is so high. Despite Federal Acquisition Rules that require security to be baked into procurements at the beginning, most times it is not. There are no penalties or even checks and balances to ensure security is part of the acquisition strategy. Microsoft's support for the Air Force should be a model for other operating systems and other software widely used by the government. Microsoft, with support from DoD and the NSA, recently issued secure server configurations, as well, extending the desktop benefits more deeply into the network.

Third, the most important ingredient in effective security automation is integration with IT automation. The Air Force success in reducing patch time came from baking security into every system configuration and into its automated IT management process. Under attack, the Air Force can change the configuration of nearly every system in minutes. That doesn't happen in agencies where security is considered a separate responsibility from effective IT management. Thus effective security in today's threat environment is a CIO responsibility – not one that can be delegated to a security officer. Only the CIO has the resources, authority and tools to implement enterprise-wide configuration management and other automation measures so critical to security.

4. Four huge unintended errors make it almost impossible for agencies to make big improvements in IT security. This Committee can fix all four

Error 1. We're measuring security the wrong way.

The predecessor to the Federal Information Security Management Act (FISMA) was written by this committee in late 2000 (under the name GISRA). It was a powerful force for improved visibility for security across government. That law, along with a continuous flow of news stories about viruses and worms, awakened government to the security issue. Once the government realized the extent of the cyber problem, it needed to act. Your committee had set a sunset date after two years. By 2002, when the law came up for reauthorization, it was time to shift from writing reports about security problems to implementing effective security solutions – based on knowledge about how the attacks work. One small change was implemented in the 2002 FISMA bill, requiring agencies to establish standard configurations. That one change did a great deal of good and actually enabled the Air Force to implement its game-changing secure configurations and other agencies to begin following the Air Force lead. But now the attacks have become much more sophisticated, and FISMA needs an even greater update. The need is supported by repeated testimony of the GAO's Greg Wilshusen in which he says that the current FISMA reporting does not measure security effectiveness.

You can make FISMA much more effective by empowering OMB to measure agencies on how well they implement and automate the controls that stop known attacks, and how well they demonstrate effectiveness in identifying and mitigating damage from attacks that get through their defenses. Reporting can be an artifact of effective automation. Progress and effectiveness should be monitored, to the maximum extent possible, electronically. The State Department CISO and CIO have begun implementing such a system – they can show other agencies how it can be done.

However, federal agencies cannot move effectively to more secure systems unless you shift the emphasis of the FISMA assessments from paper reporting to automated monitoring of essential controls. If agencies are asked to implement critical controls and to automate reporting but still are forced to produce the current FISMA paper reports, they just won't be able to do so. Two weeks ago, a federal CIO told me, "I have a CISO who always gets me to green on my FISMA grades, but the reports he produces have no impact at all on security of our computers or networks, I am setting up a separate group to do real security." This CIO can do both because of a surge of funding his organization has received from the new stimulus bill. Most CIOs do not have enough money to pay for both the FISMA reports and the important security improvements.

This committee can fix that error by authorizing and empowering agencies to move to continuous monitoring of critical controls. In moving the agencies to continuous monitoring, the most valuable asset this Committee could give the agencies is a legislatively approved way to answer the questions the Air Force asked NSA: what are the most critical controls that must be implemented first to ensure government systems are protected from known attacks and that can mitigate damage from attacks that get through? And how can agencies measure those controls reliably? You can make that happen simply by telling DHS, through US-CERT, to produce that list (with help from NSA), along with measures of effectiveness, and to keep it up to date. Only US-CERT and NSA have sufficient combined knowledge of how attacks work to make the answer useful. A project led by John Gilligan (the Air Force CIO who did so much to improve security), and sponsored by the Center for Strategic and International Studies, is already helping get such a list started. Mr. Gilligan brought together experts from US-CERT, NSA, the Department of Energy Nuclear Labs, and DoD agencies that understand offense, to define the 20 most critical security controls and to draft a consensus audit guide (CAG) that could be the starting point for transforming federal cyber security. If the government leads the way, the defense industrial base and the critical national infrastructure will willingly follow. They want to stop the attacks just as much as the government does.

Error 2. Missing the opportunity to use federal procurement to buy security "baked-in'."

Technology buyers cannot cost-effectively secure technology they purchase. Had the Air Force staff tried to implement the critical security configurations changes itself they would have had to change the configurations of 500,000 computers, one by one. The cost would have been astronomical even if the skills had been available. Instead, they purchased computers with the secure version of Windows already installed.

Further, most users of technology are unwilling to make changes to systems - even critical security changes - because they fear the changes will disable important features. Only the people who build and sell technology to government can configure that technology securely. The $70 billion in annual federal IT spending is enough to get radically better security baked-in, but most agencies - other than the Air Force - are not yet using that procurement leverage to ensure systems come with security baked in. Every new contract that is let, without specific security language in the contract specifications, is another opportunity lost and another boost for our country's enemies.

There is a particularly troubling example of this problem plaguing agencies right now. Many agencies are hiring contractors to develop web sites, often to give the public access to information about their parts of the new stimulus bill. The contractors employ programmers who do not write secure code, or who use existing code building blocks which haven't been fully vetted for security purposes, and deliver flawed web sites that may cause the agency to lose data and or even to infect visitors who come to their site. When the agency discovers the problem and tells the contractor, the contractor usually charges the agency to fix the contractor's own programming errors. In some cases the extra charges are greater than the cost for writing the original, flawed application.

This Committee can help solve this problem by instructing agencies to specify security elements in every procurement and task order. The minimum set of requirements would be that the application is configured securely, operates effectively on securely configured versions of operating systems and databases, and is free of the NSA/Mitre/SANS Top 25 most dangerous programming errors. Putting that language in the Federal Acquisition Regulations (FAR) will not work. If the requirements are not in the specific language of each contract, most contractors will not implement them.

Error 3: Allowing the claim, "one size does not fit all," to derail purchases of more secure technologies

When the government tries to use its procurement power to buy software at better prices and with security baked in, vendors often scream. "One size does not fit all." And it usually works. BUT It's wrong!

Microsoft sells one size of Windows to tens of millions of people. Cisco sells one size of IOS (Cisco's operating system inside each of its routers) to hundreds of thousands of people. Oracle sells one size of its database to tens of thousands of people. Hundreds of vendors sell only one size. One size, to all these vendors, clearly fits all.

By using federal procurement to buy securely configured systems, you do not constrain agencies from innovation or from making modifications. Instead you make them safer from the outset. The Air Force proved that. Loud claims to the contrary were dead wrong. Your Committee can encourage other agencies to do so, as well.

Error 4: Expecting DHS to manage security across the civilian government without active support from a White House Cybersecurity office.

Civilian government agencies do not work on a command and control basis across agencies. If someone from one agency tells someone from another agency to implement an action, (regardless of legislative authority), the person in the second agency is likely to say "I don't work for you. If you want me to do that, have your Secretary call my Secretary and then, when I get word from my boss, I'll think about doing what you ask." You need look no further than the federal agencies' Conficker response earlier this month, for a telling example. When the US-CERT requested status reports on important mitigation actions from the agencies, their requests were met with silence from the majority of agencies. US-CERT may have provided excellent information, but US-CERT was unable to determine whether the agencies acted effectively on that information. When an attack starts to cause real damage, that lack of control will be catastrophic.

The bottom line is that without a White House office actively and intelligently forcing the agencies to work well together, and to spend money on the right security controls, DHS will fail in its federal cyber security role. That office must have command and control over civilian federal computers in time of emergency, but there is no need to place DoD cyber security under that White House office. At DoD command and control is already in place and works reasonably well. The White House cyber security office would implement its operational control over civilian agencies only when national emergency events occur, or when agencies need to act to be ready to respond to such national security events; otherwise it would play a coordinating and monitoring role working through other parts of OMB. Unless you put the power to reconfigure and unplug computers and networks in the hands of a White House office, the nation will not be able to respond quickly or effectively to a major cyber attack.

5. If you do make these corrections in government, you will, at the same time, be making cyber security much more effective for the critical national infrastructure and the general public.

The Air Force procurement has led Microsoft to bake security into the products it sells to many other buyers. A large part of the nation's infrastructure assets are run by companies and operations that use many of the same business, database, and web applications that the government uses. If vendors step up to meet minimum government mandates on security, there will be a critical ripple effect on software development and security practices used by the private sector companies.

So if those mandates are made clearer, and agencies are authorized and empowered to purchase more secure technologies, and to automate the monitoring of critical security controls, the committee in effect will be serving to prime the pump of broader adoption of effective security practices.

In Closing

Many useful cyber security initiatives were started during the past eight years – from the common secure desktop configurations, to the information security line of business, to DNS security, just to name three. But they are not nearly enough. CSIS concluded accurately, "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration. It is a battle fought mainly in the shadows. It is a battle we are losing."

The key to turning the tide against the attackers is strategic use of federal IT procurement. If procurement is not fixed, nothing else really matters.

Tom Kellermann
Vice President of Security Awareness, Core Security Technologies
CSIS Cyber Security Commission Member
Certified Information Security Manager (CISM)

Before the
United States Senate
Homeland Security and Government Affairs Committee
April 28, 2009

Introduction

Chairman Lieberman, Ranking Member Collins and Members of the Committee, I profoundly appreciate the opportunity to address you today on these matters of cyber-security before us which are so critically important to protecting the well-being of our nation's citizens, physical infrastructure, intellectual property and economy.

Over my years of work as an information technology (IT) security practitioner for organizations including the World Bank, as an advocate for policy efforts including the Center for Strategic and International Studies Commission on Cyber Security for the 44th Presidency, and as a representative of Core Security Technologies, I've had the unique opportunity to gain detailed insight into the incredible challenges facing organizations of all kinds today, including federal agencies, in relation to the multifarious risks posed by hackers, virus-writers, state actors and a litany of other malicious operators involved in executing cybercrimes.

It is without any shade of doubt that I sit here before you determined to convince you further that the problems facing our nation today as it relates to stemming the ability of individuals, organized criminals, terrorists and foreign nations themselves to infiltrate our electronic infrastructure – for the purpose of assailing everything from our most strategic national information resources to our critical physical grid systems – cannot be understated.

Looking back at the horrible events of Sept. 11, 2001, it should be recognized that while those attacks did not leverage a heavy dose of computing assets, one important lesson that we should take from the tragedy is that terrorist groups and other state enemies can and will leverage the technologies that we as a society depend upon most to achieve their nefarious objectives. Since 9/11, it should also be noted, cybercrime has facilitated terrorist financing. As illustrated by the planning and execution of the Bali bombings of 2005, cyber-attacks have become the business model of choice for a wide range of organized elements, including international terrorists, who have employed widespread campaigns as a significant source of funding for themselves and their real-world activities.

While it may not yet be common knowledge that organized, extremist terrorist efforts are already engaging in sophisticated cyber-attacks for the purpose of damaging U.S. computing assets, and even infiltrating our critical grid infrastructures, it should be noted that these groups are also using cybercrime as a significant source of financial support. The evolution of information technology has empowered our culture with an incredible capacity to advance many of our personal, business and governmental interests, but these computing and communications tools have also a created a new, virtual and highly vulnerable frontier on which parties can carry out attacks on Americans from halfway around the globe behind the obscurity of their computers.

As many of you already know, from instances of foreign government-backed entities compromising the computing systems of our most sensitive and closely guarded national agencies, including the Department of Defense, to individuals launching computer virus attacks meant to exfiltrate the most valued intellectual property from private enterprises responsible for powering our nation's economy, the complex risks posed to the United States by the current epidemic of cybercrime should not be underestimated.

To note, the United States Computer Emergency Response Branch (U.S.-CERT) reported that there was a 40 percent increase in external computer intrusions into systems operated by the U.S. government during 2008. As far back as 2005, the Department of Justice assessed that over two-thirds of U.S. businesses had already been impacted by cybercrime. And at last year's World Economic Forum in Davos, world leaders estimated that there have already been over $1 trillion in losses suffered by the global economy via the electronic expatriation of intellectual property and financial data.

Most recently, in a study published by security consultants at Verizon Business, the experts reported that of the 90 individual breaches they investigated among customers in 2008, over 285 million records were stolen via those cyber-attacks alone.

To summarize, cyber-attacks have become a wholly pervasive phenomenon based in part on:

- Increasing connectivity and availability of assailable network, systems and applications vulnerabilities.
- The ability of cybercriminals to derive significant financial rewards through successful attacks.
- Worldwide federation between various classes of cybercriminals and malware developers.
- Nation-state, terrorist and politically driven backing of targeted cybercrime efforts.
- A lack of cohesive law enforcement around the globe.

My goal today is to outline to the Committee several areas of federal activity where I believe that more aggressive and devoted effort must be exerted to improve the ability of our government agencies, critical infrastructure providers and the many private contractors with whom they interact, to improve their ability to manage the risk posed by a hostile cyberspace.

I will also highlight several elements of enforcement currently operating under the Department of Homeland Security that deserve expanded support, both in their funding and their level of authority, to substantially improve our national cyber-defenses.

It is my contention that given this Committee's consideration and leadership, our government will not only secure itself but each of us as individuals from the range of cyber-attacks that we will continue to encounter both now and tomorrow as the adoption of technology and the subsequent evolution of the cybercrime ecosystem.

Recommendations

I. Expanding Capabilities Under DHS

One of the primary aspects of my appearance here today is to help shed light on some of the strengths and weaknesses of current enforcement mechanisms operating under the auspices of the National Cyber-security Division of the Department of Homeland Security. It is my overall assessment that while these efforts have significant value and potential in advancing important matters of cyber-defense, for the most part these initiatives have not been given sufficient financial or operational support to address their all-important mission.

Overall, while the DHS has made a good faith effort via all of these programs to improve U.S. federal standing in relation to cyber-attacks, the agency continues to struggle with major issues in its approach. Over-arching challenges that continue to detract from these efforts include:

- **Lack of Management Continuity** – many of DHS' senior cyber-security leadership positions are political appointments and by nature, result in frequent turnover of management personnel, and changes in priorities and focus of the organization's mission. Compared to other departments, DHS has an inordinate number of political appointments in leadership positions.

- **Insufficient Support Structure** – within DHS to provide fundamental functions to support cyber-security needs, such as procurement, budget/accounting, human resources, facilities, and compatible information systems.

- **Lack of Identity/Motivation** – compared to more mature departments and agencies, DHS has not realized a true *cultural identity* within its workforce, particularly in its cyber-security mission. This is an intangible characteristic, but critical to motivating and sustaining the professional workforce for the long term. One outcome of this problem is tremendous personnel turnover with political appointments and career government officers since DHS' inception.

There are three groups currently operating under DHS that I will address specifically, the U.S. CERT, the Secret Service Electronic Crimes Task Force, and the DHS Federal Network Security Branch – along with touching on the DHS Cyber-Storm incident response exercises:

1. U.S.-CERT

The United States Computer Emergency Response TEAM, or CERT, serves one of the most important roles in federal oversight of issues impacting matters of national cyber-security, both for government entities and our legions of private organizations. In researching and responding to emerging cyber-security threats ranging from virus and malware attacks to IT security vulnerabilities discovered in widely used technologies, U.S.-CERT fills the vital role of our national cyber-defense first responders.

Among the few existing efforts that successfully reach across both public and private sectors to help advance U.S. readiness for, and response to, cyber-security issues, it is my opinion that U.S.-CERT is fulfilling a critical role in providing our nation with crucial intelligence needed to stay ahead of both existing and future cyber-attacks. While there is continued emphasis being placed by executive leadership on any efforts that can be made by the federal government to create partnerships that foster closer cooperation between public and private entities to share information and expertise in the area of warding off cybercrime, U.S.-CERT is perhaps the best example of an established resource that is meeting those expectations today.

At the same time, U.S.-CERT has been limited in its ability to move beyond mere information sharing into other more dynamic operations that can provide even greater insight into cyber-security problems, based on a lack of sufficient funding and organizational authority.

U.S.-CERT needs to be the country's cyber-defense and coordination agency that has the ability to introduce private subject matter expertise to get actionable threat mitigation information to critical infrastructure and federal agencies.

2. Secret Service Electronic Crimes Task Force

Much like their colleagues at U.S.-CERT, the dedicated special agents working for the Secret Service Electronic Crimes Task Force have been doing an admirable job in helping to monitor and react to cyber-security trends. As an extension of the Secret Service's core mandate to safeguard the nation's financial infrastructure and payment systems, the Electronic Crimes Task Force has served a crucial role in aggregating vital cyber-intelligence, investigating specific cybercrime incidents, and channeling the information garnered via those efforts into subsequent attempts to identify and impede those organizations and individuals responsible for executing these illegal activities.

However, from both a resource and organizational standpoint, the Secret Service Electronic Crimes Task Force currently faces several major hurdles in order to expand its own intelligence-gathering and enforcement capabilities.

Firstly, like U.S.-CERT, the Task Force needs greater financial backing to track and pursue operators attempting to carry out cybercrime activities in our nation, and overseas, today. From providing the Task Force with the more substantial manpower and technological tools necessary to complete these tasks, to ensuring that the most qualified agents working across the Secret Service can be enlisted and retained in executing these responsibilities, the Task Force requires a higher level of support, and greater authority among its peer organizations, to deliver on its current mandate.

A specific problem that the Task Force must address is the Secret Service's operational tradition of rotating agents through frequent post transitions to maintain a fresh approach to all its matters of enforcement. While this is clearly a very useful approach in many aspects, the work being tackled by the Task Force requires the highest level of technical acumen to address the sophisticated nature of today's real-world cybercrime activities and to maintain the continuity necessary to investigate these attacks. I would specifically suggest that in addition to providing the Task Force with greater financial backing, that the Secret Service be encouraged to adjust some of its longstanding staffing functions to ensure that it has the most qualified people on the job every day dedicated to this crucial cyber-security effort.

3. Operation Cyber Storm

I would also like to call attention to the twice-completed/bi-annual Cyber Storm cyber-security defense exercises, which have provided valuable insight into the ability of government and private organizations responsible for management of critical national infrastructures to react to cyber-attacks.

As noted, these organized tests run by the DHS to assess cyber-security readiness across public and private infrastructure offer us a vital window into the ability of our nation's critical grid services providers and law enforcement communities to respond to major cyber-attacks. However, to permit us even greater insight into the specific strengths and weaknesses in these areas, and understand how critical infrastructure (specifically energy, telecommunications, financial and health IT systems) stand up in the face of widespread and targeted campaigns, the Cyber-Storm exercises must be expanded, with participation from crucial private entities transitioned from voluntary to mandatory status.

In addition to requiring organizations responsible for critical grid infrastructure to take a more active role in simulating cyber-attacks, they must be pushed to participate in these exercises on a frequent and regimented basis. I would also suggest that these exercises must be altered to be less oriented toward check-box, paper-based requirements and expanded into more dynamic, realistic emulations of real-world cyber-attack conditions. Specifically, these tests should become focused less on issues of infrastructure resiliency and service performance, and encompass more of the highly sophisticated staged infiltration techniques being employed by today's heavily organized cyber-criminals and state actors.

4. NCSD Federal Network Security Branch

Even more so than the two previously cited organizations addressing cyber-security under DHS management, the Federal Network Security Branch finds itself in a challenging position in terms of fiscal backing and authority. For, while the Branch currently maintains a worthy desire to address its goals of hardening U.S. network computing infrastructure against cyber-attack, the organization has not been provided with the necessary support to deliver on its strategic objectives. That said; the Branch has done a tremendous job in maximizing the resources that have historically been placed at its disposal.

A specific example of the many organizational challenges faced by the Branch can be found in its oversight of Presidential Directive 23, which addresses governance of Network Operations Center (NOC)/Security Operations Center (SOC) operating standards. While this management function represents a substantial opportunity for the Branch to have a significant impact in improving the capabilities of these installations to help our nation predict and respond to emerging cyber-security issues, it has not been granted the necessary authority to foster the needed defense-in-depth protective IT mechanisms needed to empower these operations.

One of my specific criticisms of the manner in which the NCSD Federal Network Security Branch is currently operated is that its initiatives have been focused too heavily on enforcement of policies related to regulatory compliance based on existing FISMA requirements. An example of this reality can be found in its efforts around the advancement of the Trusted Internet Computing (TIC) program, an effort mandated in an OMB memorandum issued in November 2007. This memorandum was meant to optimize individual external connections, including Internet points of presence currently in use by the federal government of the United States, to address security issues.

While the Branch has played a vital role in forwarding this important infrastructure hardening enterprise, it has not been able to serve in a lead role in driving expansion and enforcement of TIC, which has deteriorated the initiative's overall ability to produce substantive, measurable improvements to our national cyber-infrastructure.

I would suggest that in re-addressing the National Cyber Security Divisions efforts, that the Federal Network Security Branch be empowered to act as the lead when driving TIC and similar programs. A red teaming penetration testing capability should also be established within the Federal Network Security Branch to provide greater situational awareness of weaknesses in civilian agency network security postures.

II. Realizing IT Risk Management via Red Teaming Security/Penetration Testing

As evidenced by specific campaigns carried out against federal agencies in recent years, and further illustrated by trends emerging on the larger cybercrime landscape, a lack of situational awareness and an inability to predict the specific methods being utilized by electronic assailants of all archetypes has been one of the most significant failures in stemming the tide of successful attacks.

While organizations across the federal space, as well as the private sector, have gone to great lengths to employ layered defensive mechanisms aimed at preventing specific classes of threats from infiltrating their IT systems, clearly, based on the successful campaigns that we know of – such as the set of coordinated cyber-attacks emanating out of China beginning in 2003 labeled "Titan Rain" – which compromised assets at the DoD, NASA and Sandia National Laboratories, as well as those of federal contractors – these existing perimeter defenses have been proven vastly insufficient. And as we know there are many more incidents that have occurred and that have not been reported publicly.

To address this dire reality, which has been highlighted most recently by widely publicized hacking of the U.S. energy grid and electronic data theft carried out against private merchants such as Heartland Payment Systems, which saw thieves make off with millions of its sensitive customer payment card records, the federal government must expand the Federal Information Security Management Act (FISMA) to compel all agencies to undergo more frequent internal assessments to gauge their risk to cyber-attacks.

Agencies must embrace the results of exercises including "Operation Eligible Receiver" – an audit of the Pentagon's exposure to cyber-attack ordered by the Joint Chiefs of Staff in 1997 – through which internal security testing specialists, dubbed Red Teams, found it exceptionally easy to circumvent existing defenses to compromise and infiltrate some of the government's most heavily guarded IT systems – to better assess their own exposure to hacking techniques of all varieties.

Specifically, agencies must be required to conduct regular, extensive security audits of their IT systems using Red Team penetration testing methodologies to gain a more precise fix on where their most significant weaknesses lie by emulating the same tactics as those being employed by cybercriminals. I would suggest that these Red Team exercises be carried out on at least a quarterly basis due to the dynamic nature of the cyber-threat environment.

These quarterly security and IT systems penetration tests (as defined by NIST special document 800-53A, Appendix G) must be applied to all federal networks and computing assets, as well as those of critical infrastructure providers across the energy, telecommunications, finance and health sectors, among others, to empower both government and private organizations to gain a better understanding of where they are most vulnerable to real-world attacks. Using classic risk management practices via the employment of techniques that mirror those used by attackers in a safe, controlled manner, those critical vulnerabilities that are identified via this process can then be remediated.

In addition, I would ask this Committee to consider the creation of systems of accountability, including penalties, for those organizations found to be unable to properly address their critical vulnerabilities.

By compelling federal agencies and their business partners to engage in this proactive security testing, and specifically conduct regular internal Red Team penetration testing assessments, these organizations will be able to both identify their most pressing instances of IT risk to ward off attacks, and to create concrete benchmarks that they can refer to frequently over time to mark their progress in improving their security posture. Subsequently, this will also allow organizations to more wisely allocate finite IT security resources.

III. Securing the Managed Service Supply Chain

The infamous breach of DHS three years ago was based on a lack of standard of care and due diligence enforced by a third-party managed service provider. The previously noted 2008 Verizon Data Breach Report noted that 39% of breaches were a result of hackers transiting/island-hopping through strategic partner networks. For these reasons, it is imperative that we grapple with the systemic risk posed by outsourcing which permeates our digital ecosystem.

The reason why global businesses open offices in New York City and pay astronomical rent is because they have trust and confidence in the safety and soundness of U.S. markets. These businesses have faith in the rule of law, the enforcement of contracts and the security of the physical U.S. marketplace.

This real world phenomenon can someday manifest itself in cyberspace if political leadership challenges the Web hosting, data warehousing and many other managed IT service providers serving the federal market to improve their standard of care per cyber-security.

In order to promote and create a secure U.S. cyber-ecosystem, this Committee should mandate that all entities who provide Managed Information Services of any sort to the U.S. government or providers of critical infrastructure (as defined by the NIPP) sign Information Security Service Level Agreements (ISSLAs) which include at a minimum a specific standard of care. The agreements must require that these service providers:

- Verify that the legal requirements to which service providers are contractually obligated to provide security are compatible with NIST 800-53.
- Outline and review their incident response plans prior to any movement of data or provision of service.
- Confirm that their policies and agreements regarding security breaches include customer notification on a timely basis (within one hour) and maintain the right to test their incident response plans on an annual basis.
- Confirm that service providers have adequate data backup facilities which are also regularly tested for security vulnerabilities.
- Conduct Red Team penetration testing of their network security posture, and verify whether they have sufficient layered IT defense mechanisms (NIST 800-53A, Appendix G serves as excellent guidance on this matter).

We must use federal acquisitions policy to require these service providers comply with all of these individual requirements. Those organizations that cannot or will not comply in this manner should have their contracts revoked.

This Committee might also consider a federal bill giving tax credits to all commercial entities that currently are FISMA compliant, as well as offer tax credits to those organizations who maintain ISSLAs with third parties and strategic partners in 2009.

IV. Closing Remarks

In summary, while the national and worldwide cybercrime pandemic is currently scaling in an exponential manner, I would submit that significant gains can be realized throughout the federal government today via the political application of more aggressive attention and investment on the part of involved stakeholders. The CSIS Report noted that since markets have failed to evolve in the face of unprecedented market forces, new public policies are necessitated.

By aligning our organizational assets and international relationships more effectively, and adopting a more comprehensive risk management approach to securing our critical national computing and communications assets, the United States can turn back the tide of cyber-attacks.

In this dark hour we need strong bipartisan leadership. The dramatic increase in cyber-attacks necessitates action. The recent 60 Day Cyber Review developed by Melissa Hathaway, the Obama Administration's acting director for cyberspace, represents a great starting point for the Administration to lead our nation's cyber security efforts. However, it is paramount that this Committee understands that it too can serve a fundamental role in defending our nation's critical infrastructures.

I appreciate your consideration of my statement and your public service.

Sincerely,

Tom Kellermann, CISM
Vice President of Security Awareness
Core Security Technologies

Post-Hearing Questions for the Record
Submitted to the Honorable Stewart A. Baker
From Senator Joseph I. Lieberman

"Cyber Security: Developing a National Security Strategy"
April 28, 2009

1. The National Security Agency (NSA) currently offers the Department of Homeland Security (DHS) technical support for its cyber security activities.

   a. Do you believe that the NSA's domestic responsibilities should expand beyond that supportive role?

   Broadly speaking, no. DHS will need technical support for some time, but it makes sense for DHS to have responsibility for the mission, rather than asking NSA to undertake that role.

   b. Why is it important to have open civilian agencies involved in cyber security? Why can't we secure our nation from cyber attack through intelligence and military efforts alone?

   Civilian agencies, especially those focused on law enforcement and internal security, often have an appreciation for the limitations imposed by domestic law and policy that are more nuanced than the perspectives of the military or intelligence agencies.

   c. Please describe what you believe to be the ideal relationship between DHS and NSA.

   As I said above, DHS will need technical support for some time, and there should be no time limit on the most sophisticated support, which will always be a strength of NSA's. In addition, NSA's intelligence activities should tightly support DHS, because foreign nation-state attacks on the US government and private sector will require as much insight into foreign tactics and capabilities as we can get.

2. The concept of establishing a new White House office to coordinate cyber security policy raises questions about what specific responsibilities the office will assume and the potential lack of congressional oversight.

   a. I'm concerned about a lack of transparency and oversight if too much responsibility is moved to the White House – which has been a problem in this area in the past. If a new White House office is created to lead cyber security policy, do you believe it needs to subject to some form of congressional oversight?

   I'm skeptical; I fear that institutionalizing Congressional authority over the office (making it subject to confirmation by the Senate, giving it a statutory charter) will reduce its clout inside the White House, because it will lead to questions about whether the office is carrying out the President's priorities or trying to serve two masters.

   b. The White House has also recently created the position of Chief Technology Officer, and gave the E-Gov Administrator additional responsibilities as Federal Chief Information Officer. Given that security needs to be considered when making decisions relating to information technology, would the creation of another office create more confusion and make effective management more difficult? How could these offices effectively work together?

   Coordination with all these offices will be a major problem for the cybersecurity office. Appendix A contains a lighthearted excerpt from my blog that shows the risk posed by the complex oversight and coordination structure dealing with this issue.

3. While DHS was given cyber security responsibilities in the Homeland Security Act of 2002 (P.L. 107-296), the arm of DHS entrusted with those responsibilities -- the National Cyber Security Division (NCSD) -- was not given adequate resources or authority to accomplish its mission. In recognition of this gap, NCSD's budget has more than tripled since 2007 under the Comprehensive Cyber Security Initiative (CNCI). However, NCSD still faces many challenges such as attracting qualified staff and lack of authority over any of the entities it's supposed to help secure.

    a. What needs to be done to help DHS execute its cyber security mission? Does it need more resources? More authority? A change in organizational structure? More hiring flexibilities? Please explain.

    Hiring flexibility is perhaps the most immediate need, in my view. I would also consider reforming the "suitability" standards imposed by DHS's security office. These have become a major constraint on hiring.

    b. Much of the additional funding NCSD has received is funding the expansion of Einstein, an intrusion detection system meant to monitor the networks of federal civilian agencies for intrusions. Is this a good use of funding? If not, where would you recommend investing in order to protect federal networks?

    Einstein is at bottom just another name for a commercial product – intrusion detection and prevention. I'm skeptical about buying a lot of hardware under the brand name Einstein, but it is clear that the government needs to do a better job of centralized and uniform intrusion prevention. That, rather than buying boxes with the Einstein label, is where I would put the emphasis.

4. Most federal cyber security efforts to date have been focused on securing government networks. While this is an important endeavor, it's really only a small part of the battle. The vast majority of cyber infrastructure is privately held, yet the impacts of any disruption, destruction, or misuse of these systems are not remotely private. These networks control every aspect of our lives – our electricity, water supply, and bank accounts, to name a few examples. Yet the task of ensuring the security of these systems is challenging since the government does not own them.

    a. Can you please discuss some of the potential impacts of a cyber attack on key critical infrastructure sectors?

    It could be devastating. Power and gas lines in parts of the country could go down. Financial systems could become unreliable. Phone systems could fail.

    b. How do we best engage with the private sector to increase cyber security across the private networks?

    I would start with existing regulatory systems, focusing regulators' attention on improving computer security in areas such as power, gas, telecom, and banking.

5. A Center for Strategic and International Study (CSIS) Commission report found that, "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives." Do you believe that some level of regulation is needed to secure cyberspace? If so, in what specific area? Do you have any thoughts on what that regulation would look like?

    Private institutions will adopt security measures that are cost effective for them. If the theft of data from their systems has a low cost, or if they are not sure what security measures will prevent the theft, or if the security measures cost more than the theft, private institutions are not incentivized to adopt more security measures. Similarly, few private institutions make investments to ward off nation-state attacks that may occur in some future contingency. These are all areas where there is a risk of market failure.

The harder question is how to address that market failure without stultifying regulation. Without purporting to have a complete answer, I suspect we would be better off with something faster and less formal than regulations, or even OMB-approved guidance, setting out specific security measures to be adopted.

6. One sector of particular concern is the electric sector. Not only does every aspect of economy and way of life rely on electricity, but cyber vulnerabilities with the sector have been well documented. Currently the federal government has no authority to compel basic security practices within the electric sector regardless of how severe a threat we encounter. The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) have both come to Congress supporting additional federal authorities in this area. Do you support legislation providing FERC and DHS additional authority to ensure the security of the electric sector from cyber attack?

I haven't looked at specific proposals, but I agree that there is a threat and that DHS, FERC, and NERC need clear authorities to address it.

7. Cyber criminals are currently stealing hundreds of millions of dollars and often these thefts go undetected by the general population.

   a. Why don't we hear more about these thefts? Who ends up footing the bill when these funds are stolen from an ATM or a bank?

   Typically, as I understand it, the financial institution bears these costs, even when the law might allow the institution to pass those costs on to customers.

   b. Are financial institutions doing everything they can to prevent these thefts?

   Where the financial institution bears the costs, it has a strong incentive to keep thefts down to a bearable level.

8. The United States is under constant cyber attack. Often times we don't know to a high degree of certainty who is attacking us. This is a new concept in warfare as it's usually fairly easy to trace a physical attack.

   a. Is a cyber attack an act of war?

   If it causes enough harm, it surely is an act of war.

   b. If so, how should we respond – especially if we're not sure who the attacker is?

   The problem is not whether it's an act of war; the problem is figuring out who we're at war with. If we cannot attribute the attack to an identified attacker, then we should be cautious about launching a counterattack. At some point, however, a nation that provides a sanctuary for attackers (e.g., by not shutting down their systems and arresting them) becomes responsible for the harm that they do.

9. One tool that the federal government has in its cyber security arsenal is its large buying power. Many of the problems that we have seen in federal government cyber security have been the result of either purchasing insecure software or problems with managed service providers. We've heard some testimony today about not only the need to require more security from our contractors to protect government systems, but also that such reform would better protect critical infrastructure and the general public by encouraging the IT providers to build this security into all their products.

   a. How we can get to a point where government is buying more secure products and what challenges we face getting to that point?

   This is a big problem. It is my observation that those who buy products for the government feel that they are paying more because of "social responsibility" limits on competition, so

they've been resistant to a broad new mandate to buy secure products. But in fact, we will have to add security to the process.

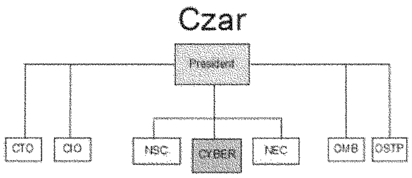
b. How do we reform the process so that these products keep up with an ever changing threat? **We could start by creating a clear requirement to exclude from competition companies whose reliability and security are suspect. That could require reliance on classified information in some cases.**

Appendix A from "Skating on Stilts" blog:

Evolution of the Cyber " Czar " in Four Easy Steps

Remember the original proposal for a cyber "czar" who would bring coherence to all network security activities across the government? The lines of authority would be crisp and clear. The cyber czar would report directly to the President as a sign of his or her authority. He or she could just walk into the Oval Office all alone and tell it like it is.

Need an organization chart? Piece of cake:

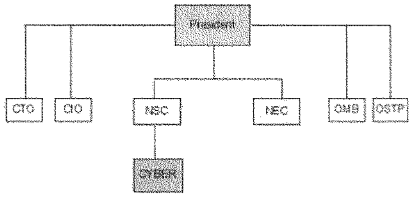


Well, on second hand, that may not quite work. Cyber security is a matter of national security, and the departments need to weigh in on cyber issues through existing channels.

But, really, that's no problem. We'll put the cyber czar into the National Security Council. There will still be one voice and one chain of command for all cyber security issues. It will just go up through the National Security Adviser. And, of course, the National Security Adviser will escort the czar into the Oval Office.

Guess we'll have to change the title, though:

Deputy Czar

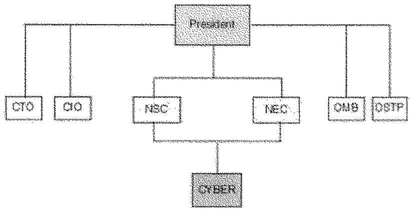


Wait! We reckoned without Larry Summers and the National Economic Council. We don't want national security types running amok and wrecking the most innovative sector of the economy with incautious regulation in the name of security.

Anything the cyber czar does really needs to be subject to the full discipline of an economic review. Make the position part of the NEC process too. The czar can report up through both the National Security Adviser and the National Economic Adviser. Once the czar has found a position that both advisers can agree on, well, they'll both go into the Oval Office with him, just to keep him honest.

Okay, with two bosses, perhaps another description of the position is in order:

Deputy Assistant Czar



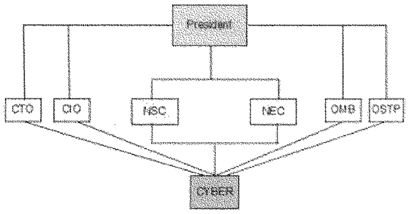
Hold the presses! NEC isn't the only White House office that wants to assert its prerogatives. What about OMB, which traditionally sets budget standards and measures departmental compliance with White House priorities? What about the CIO and CTO positions that the President just filled with such fanfare? They aren't chopped liver. Cyber security is all about information and technology. Oh, and the Office of Science and Technology Policy -- what is cyber security policy if it isn't science and technology policy?

Better give them a veto over what the cyber czar says to the President, too. We'll have to move the meetings out of the Oval Office, of course, but there's bound to be an auditorium nearby.

With these changes, we'll need a new org chart and a new title, but surely there's a czar who could serve as a role model for the position. ... Um ... hang on ... it'll come to us ...

Yes! We've got it:

Czar Nicholas (1919)



Post-Hearing Questions for the Record
Submitted to James A. Lewis
From Senator Joseph I. Lieberman

"Cyber Security: Developing a National Security Strategy"
April 28, 2009

1. **In your written testimony, you stated that there is still debate within the Administration as to "how strenuously the U.S. should protect its cyber networks." Can you elaborate on this point? Who is the debate between and what is the argument for not protecting our cyber networks?**

Cybersecurity has been, so far, a second tier priority for the administration. Concerns that too great an emphasis on security would have damaging economic effects explains this in part. The administration has identified increased use of the internet and digital technologies as crucial tools for recover and future growth (hence the ill-conceived program to subsidize broadband to undeserved rural areas). This concept for the use of IT is in itself a reasonable assumption – greater use of information technology explains a significant portion of economic growth before the recession – but various offices in the White house asserted that the powers and stature of a White house coordinator must be diluted and constrained to avoid any risk to the economy.

It is interesting to compare this with climate change. Mitigating the effects of climate is important, and it also holds real economic risk. Despite this, the White House was able to quickly appoint an Assistant to the President for climate change. The conclusion is that climate change was important enough to move quickly and that the Administration believed it would be able to design a sophisticated approached that mitigated the problem while minimizing economic damage. The same assumption should have been applied to cybersecurity, but it was not because of a debate over both substance and turf.

2. **The National Security Agency (NSA) currently offers the Department of Homeland Security (DHS) technical support for its cyber security activities.**

   a. **Do you believe that the NSA's domestic responsibilities should expand beyond that supportive role?**
   b. **Why is it important to have open civilian agencies involved in cyber security? Why can't we secure our nation from cyber attack through intelligence and military efforts alone?**
   c. **Please describe what you believe to be the ideal relationship between DHS and NSA.**

Technologies developed by NSA could substantially improve cybersecurity if deployed widely across government and 'backbone' commercial service providers. Since these technologies involve the monitoring of traffic (to detect malicious code) they pose serious civil liberties concerns and cannot be deployed under our current laws. If we cannot assure adequate oversight and minimization of monitoring, we deny ourselves the technologies that already exist to improve cybersecurity, but this monitoring cannot come at the expense of rights assigned by the Constitution that restrict the ability of government to monitor private communications.

NSA, as an intelligence agency, is not well positioned to carry out domestic functions and a supportive role for DHS, similar to the cooperative role NSA plays with the FBI, is probably the best approach (e.g technical advice within the framework of DHS authorities and oversight).

3. **The concept of establishing a new White House office to coordinate cyber security policy raises questions about what specific responsibilities the office will assume and the potential lack of congressional oversight.**

    a. **I'm concerned about a lack of transparency and oversight if too much responsibility is moved to the White House – which has been a problem in this area in the past. If a new White House office is created to lead cyber security policy, do you believe it needs to subject to some form of congressional oversight?**
    b. **The White House has also recently created the position of Chief Technology Officer, and gave the E-Gov Administrator additional responsibilities as Federal Chief Information Officer. Given that security needs to be considered when making decisions relating to information technology, would the creation of another office create more confusion and make effective management more difficult? How could these offices effectively work together?**

The lack of Congressional oversight is a serious problem but the lack of progress over the last decade in securing our nation's digital infrastructure is an even greater problem and one that poses an immediate and direct threat to the security of the United States. The failure to adequately respond to this problem has been one of the greatest failings of this government under several administrations. If the choices are oversight and no action in a crisis or no oversight and action – and those appear to be our choices at the moment, I prefer the latter.

Neither the CTO not he CIO have security as a primary function. Additionally, if we accept that cyber activities are now a major problem for national security and a part of any international conflict, and that an adequate national approach must integrate cybersecurity into the larger framework of diplomatic, military and intelligence operations supervised by the National Security Council, these offices are not the right ones for the job. Our primary opponents in cyber space are foreign intelligence services and militaries, and sophisticated cyber criminals locate din a few countries. Countering their efforts is not the primary responsibility of a CIO or CTO. Technology and organization are part of what is needed for better cybersecurity, but they are not in themselves sufficient and we need to stop approach cybersecurity as a technology issue – it's like assigning the lead for air defense to the FAA.

4. **While DHS was given cyber security responsibilities in the Homeland Security Act of 2002 (P.L. 107-296), the arm of DHS entrusted with those responsibilities -- the National Cyber Security Division (NCSD) -- was not given adequate resources or authority to accomplish its mission. In recognition of this gap, NCSD's budget has more than tripled since 2007 under the Comprehensive Cyber Security Initiative (CNCI). However, NCSD still faces many challenges such as attracting qualified staff and lack of authority over any of the entities it's supposed to help secure.**

    a. **What needs to be done to help DHS execute its cyber security mission? Does it need more resources? More authority? A change in organizational structure? More hiring flexibilities? Please explain.**
    b. **Much of the additional funding NCSD has received is funding the expansion of Einstein, an intrusion detection system meant to monitor the networks of federal civilian agencies for intrusions. Is this a good use of funding? If not, where would you recommend investing in order to protect federal networks?**

DHS is the most junior member of the national security community and its national security capabilities are limited. Even civilian agencies appear to believe that responding to DHS requests are optional. I would not try to strengthen DHS's role in national security – it lacks expertise, experience, and analytical capabilities. DHS is primarily a law enforcement agency and this limits its national security role. However, DHS is the best agency for coordinating the security of dot-gov networks, in the same way that DISA is responsible for the dot-mil networks. Providing DHS similar authorities that would allow it to require mandatory action by civilian agencies to secure their networks would be a useful first step.

5. **Most federal cyber security efforts to date have been focused on securing government networks. While this is an important endeavor, it's really only a small part of the battle. The vast majority of cyber infrastructure is privately held, yet the impacts of any disruption, destruction, or misuse of these systems are not remotely private. These networks control every aspect of our lives – our electricity, water supply, and bank accounts, to name a few examples. Yet the task of ensuring the security of these systems is challenging since the government does not own them.**

   a. **Can you please discuss some of the potential impacts of a cyber attack on key critical infrastructure sectors?**
   b. **How do we best engage with the private sector to increase cyber security across the private networks?**

A serious cyber attack would disrupt critical services for an extended period of time, perhaps shutting off electrical supplies, fuel pipelines, or dislocating the financial system. The United States has not faced such attacks, but that is only because the political circumstances that would justify such attacks by other nations have not yet occurred and because non-state actors have not yet acquired the necessary capabilities.

U.S. cybersecurity policy has been markedly shaped by ideology, and this in large measure explains its failure. Our policy has been faith-based: we have faith that the private sector will do the right thing. There are some easy parallels to consider. Our approach to working with the privates sector in cybersecurity is similar to an approach to airline safety that says, we do not need the FAA to develop standards and inspect plane, because airlines own the majority of airplanes and it is in their business interest to offer safe services. We do not need to inspect food or drugs because again, market forces will lead companies to do the right thing. This is obviously blather, but it is a blather we have tolerated for more than a decade when it comes to securing networks.

The notion that companies would change their behavior and spend more on security if the government shared information with them has also been tested and failed. The private sector en toto will only do enough for national security if they are required to by regulation. Companies will take public private partnership seriously if there is some skin in the game – and that requires regulation. This may, however, be too hard for the United States and this could require a 'second-best" strategy that accepts continued vulnerability and loss and asks how to compensate for this.

6. **A Center for Strategic and International Study (CSIS) Commission report found that, "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives." Do you believe that some level of regulation is needed to secure cyberspace? If so, in what specific area? Do you have any thoughts on what that regulation would look like?**

Frankly I am a bit gloomy on this. We now what the problem is; we now what is required to fix it, but we are politically unable to carry this out. One way to think about regulation in cyberspace is to compare it to passenger aircraft. If I said that we do not need to FAA to regulate how airlines maintain their aircraft, since it is in their business interest to do an adequate job, you would think I was insane. This is how countries like Malawi and Yemen provide for air safety, and it is what the US does for cybersecurity.

7. **One sector of particular concern is the electric sector. Not only does every aspect of economy and way of life rely on electricity, but cyber vulnerabilities with the sector have been well documented. Currently the federal government has no authority to compel basic security practices within the electric sector regardless of how severe a threat we encounter. The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) have both come to Congress supporting additional federal authorities in this area. Do you support legislation providing FERC and DHS additional authority to ensure the security of the electric sector from cyber attack?**

This legislation is essential. We should always try to minimize the regulatory burden on the economy, but there are some functions – safety and security being two of them – that the market will never supply adequately. Electrical grids are a routine target for attack and we as a nation have not done enough to defend them. A failure now to make a greater effort to secure the electrical grid will guarantee disruption in some future attack.

8. **Cyber criminals are currently stealing hundreds of millions of dollars and often these thefts go undetected by the general population.**

   a. **Why don't we hear more about these thefts? Who ends up footing the bill when these funds are stolen from an ATM or a bank?**
   b. **Are financial institutions doing everything they can to prevent these thefts?**

Companies worry about reputation damage. This is a reasonable concern, but the result is that they conceal their losses. Consumers pay for these losses in the form of higher charges. How much should be done to limit the losses is a business decision for companies. If more security costs more than the what is being lost, they chose to "eat" the cost. This will eventually change when the cost of not responding is greater than the cost of better security.

Financial institutions can only do so much. Decreasing cybercrime depends largely on cooperation among nations to enforce laws and shrink sanctuaries. This is a government function that banks cannot duplicate. Financial institutions could do more to lobby their government to take the cybercrime problem seriously.

9. **The United States is under constant cyber attack. Often times we don't know to a high degree of certainty who is attacking us. This is a new concept in warfare as it's usually fairly easy to trace a physical attack.**

   a. **Is a cyber attack an act of war?**
   b. **If so, how should we respond – especially if we're not sure who the attacker is?**

This answer is excerpted from a forthcoming CSIS report, "A Preliminary Note on the "Korean" Cyber Attacks and the Implications for Cyber Conflict."

If has been a few weeks since the end of the primitive network attacks against networks in the United States and South Korea and no one has yet taken credit. The attacks were at first widely attributed to

North Korea, but there is no conclusive evidence as to who was responsible. This failure of attribution suggests several conclusions on the nature and state of cyber conflict.

First, the response options for the United States were extremely limited. The United States could have made North Korea the target for counterattack on general principles – they are belligerent and an attack could be justified even if they were not responsible for this particular incident. No serious person advocated this, however. Starting a conflict with North Korea in response is unthinkable. In fact, an astute third party might have made it look like North Korea in order to lure us into an unnecessary and damaging dispute. The use of botnets for an attack – thousands of remotely controlled third party computers –also complicates any response. Botnets provide a greater degree of anonymity and guarantee that if there is a counterstrike against an attacking computer, it is almost certain also to involve a strike on an innocent and unwitting third party.

Weak attribution makes traditional deterrent capabilities – those based on counterforce or countervalue attacks – largely irrelevant. Since an opponent's anonymity reduces the risk of them suffering a counterattack, the deterrent value of such attacks are also reduced. Deterrence is further complicated by the problems of collateral damage – to strike North Korea with cyber attacks we would have had to traverse networks and fiber optic cables that go through Japan and China (and probably California), possibly damaging them.

Deterrence relies on changing the opponent's calculus of the benefits and costs of an attack. The threat of counterstrike was the basis of deterrence in the Cold War. It is no longer adequate. In the Cold War, there was symmetry in vulnerabilities – each side had cities and populations that the other could hold hostage. That symmetry no longer exists. The United States is far more dependent on digital networks that its opponents and this asymmetric vulnerability means that the U.S. would come out worse in any cyber exchange.

There was clear attribution in the Cold War (although some scenarios explored the possibility of an "anonymous bomb" from a third party to trigger war between the U.S. and U.S.S.R.) that allowed for both credible directed threats and for "signaling" and tacit understandings between opponents on "redlines" and thresholds. We do not have that clarity in cyber conflict, complicating any effort to "signal" an opponent. Asymmetric vulnerability, weak attribution and unknowable collateral damage limits our ability to make a credible threat against an opponent in cyberspace.

The problems for deterrence are compounded by the lack of international norms on cyber conflict and lack of robust doctrine. An opponent's calculus of the benefits of an attack will be shaped, to varying degrees, by their concern over the reaction of the international community. Norms can limit the scope of conflict. The lack of generally accepted international norm for cyber conflict eliminates this "braking" effect and reduces the political cost of cyber attack. One question to consider is whether we have been too quick to strip cyber conflict from its political context and treat is as a largely technological and impersonal phenomenon.

Given the limitations for counteroffensive action, cyber conflict stands the old bromide on its head: the best offense in cyberspace is a good defense. By reducing the likelihood of success for an opponent in launching a cyber attack, we change the deterrent calculus in ways that benefit us and in ways that are not achievable by threatening counteroffensive actions.

These limitations also affect the ability to dominate or deny an opponent access to cyberspace. Degradation of an opponent's military networks and information, or the networks that support critical infrastructure, is a legitimate military objective,[1] but the degree of interconnection with third parties

[1] The simple rule being that if it is legitimate to attack a target physically, it is legitimate to attack it using cyber weapons as well

complicates the use of cyber attacks. Inadvertent damage to third party networks during a counterattack carries high political risk that has to date been underestimated in many discussions of cyber warfare.

Cyber conflict will not be "clean," where only combatants are present in the area of operations. Instead, cyber conflict will take place in an crowded environment where combatants are closely connected to noncombatants, including allies, friends and neutral third parties. Combatants and noncombatants may even interdependent connections with each other in cyberspace, so that an attack on a legitimate target may unavoidably damage a neutral party. This means that the political consequences of cyber attack are greater and require greater attention from the political leadership before action is authorized.

An opponent who exploits this interconnectivity and the availability of third party commercial service to develop resilient architectures may be able to evade or limit the ability to deny the use of cyberspace. Resiliency could be produced by the development of redundancy in data and services or by architecting networks in ways that make them easier to defend. Given time, of course, these approaches could be defeated by a determined and well-resourced opponent.

The political consequences of cyber conflict have probably been underestimated by most participants. One precedent to illustrate this kind of underestimation is the German decision to wage unrestricted submarine warfare in 1916 and attack neutral ships. This provided some tactical advantage but was an immense strategic blunder. Another precedent may lie with Chinese cyber espionage operations carried out by a wide range of official and commercial entities in that country. These operations have been tolerated if not approved by the government, but they now may threaten relations with several major trading partners and the Chinese government may need to develop new modes of oversight and control to minimize political risk.

Cyber conflict as it is currently waged falls largely outside the space of military action. That the military has only a limited role in cyber conflict as it is currently waged does not mean that military forces should not develop cyber capabilities. Cyber attack will form part of any future conflict. The primary requirement is defensive – the U.S. military relies more on networks and information than others do, and the consequences of any exchange are again likely to be asymmetric – the U.S. will suffer more if it does not have a preponderant advantage in defense. But as part of the larger deterrent effect of having a capable national military force, that force must be organized and equipped to engage in offensive actions in cyberspace.

The cyber incidents in early July did not rise to the level of an act of war. They were annoying and, for some agencies, embarrassing, but there was no violence or destruction. Escalating our response to involve the use of kinetic weapons would have been unjustified. Attacking North Korea's networks would be largely pointless – their economy does not depend on them. In fact, there is no role for military action or the military in a response to the "Korean" attacks. Cyber conflict as it is currently waged falls largely outside the space of military action.

Weak attribution is the primary reason for this, but a lack of clarity on what kind of cyber attack justifies a military response also limits the scope for military action. There are implicit norms and thresholds for cyber attack that have merged in the last few years, but they are too imprecise to define the boundaries for military response. There is no international consensus (and barely any discussion) of what are the thresholds for cyber conflict or the paths for escalation of such conflict (in either the cyber or kinetic realm).

Most incidents in cyber conflicts do not rise to the level of an act of war. Cybercrime is not rise to the level of an act of war, even when there is state complicity, nor does espionage – and crime and espionage are the activities that currently dominate cyber conflict. The individuals and nations that engage in these activities do not think of themselves as waging war against the United States or even engaging in practices that are outside the scope of normal international behavior (again, a problem reinforced by the lack of norms). If a nation catches a spy, there is an increase in tension, it may expel an attaché, or a protest filed, but we do not respond with military action.

An action in cyberspace that is produces the equivalent effect as sabotage begins to rise to the level of an act of war. It would be a serious matter if a nation slipped a commando team across our border and it blew up a pipeline or power station and a similar action in cyberspace would justify the same level of concern. At a minimum, we can use this to begin to define a serious cyber attack that could justify escalation as one that disrupts critical services for an extended period of time, perhaps shutting off electrical supplies, fuel pipelines, or dislocating the financial system. The United States has not faced such attacks, but that is only because the political circumstances that would justify such attacks by other nations have not yet occurred and because non-state actors have not yet acquired the necessary capabilities.

Ultimately, the decision as to whether something is an act of war rests with country's political leaders. For example, would it be an act of war if instead of cyber attacks, the North Koreans had hijacked a U.S. Navy vessel off the high seas, killing a few sailors, towed it into port, pillaged the ship and imprisoned the surviving crew? The answer is it depends – in this case (the 1968 attack on the USS Pueblo) the U.S. chose not to retaliate with military action. Political leaders will likely want precise information on attribution and on collateral damage before authorizing any cyber counterstrike, and even with this information they may decide that in the larger strategic context, the risks of military action outweigh the benefits, or that there are alternative courses of action that are more beneficial.

This suggest that there can be no reflexive rules of engagement for counterattack in cyber conflict. Some navies have rules of engagement that give the commander the discretion to fire back when his or her ship is fired upon, without prior approval from higher authorities. This sort of rule is not possible in cyberspace, since unlike a naval vessel that can identify who is attacking it and can take actions to limit collateral damage, a counterstrike in cyberspace is likely to lack clear attribution and clear scoping of the side effects on neutral parties.

The United States was hampered in considering responses to the recent attacks by the lack of an adequate national doctrine for cyber conflict. An adequate doctrine would define evidentiary requirements for response, pair attack scenarios and possible counters, describe a process for escalation in response, and clearly lay out the approval process for response and escalation. Most importantly, doctrine would define the threshold for serious attack that would justify consideration by the political leadership of an offensive action by the United States in response. A public doctrine would even have some deterrent effect (by describing the risks a potential attacker would face in response) and could help shape international opinion on cyber conflict in ways that are favorable to the United States.

The pressure to develop doctrine that allows for a rapid response has distorted thinking about cyber conflict. That an attack occurs in milliseconds does not mean that the response needs to occur with equal rapidity. First, the idea than an attack occurs in milliseconds is wrong. Usually days, if not weeks, of planning and reconnaissance have going into preparing for an attack. In this, cyber attacks are not that different from other advanced weaponry, where an exchange of fire lasting minutes is preceded by hours or days of planning, maneuvering and reconnaissance. One possible shortcoming of the American cyber defense effort is the failure to adequately utilize intelligence collection that would detect this opponent planning and reconnaissance – there is little that can be done when the packet actually arrives, but much to be gained in looking at opponent's networks and in mapping their doctrine, capabilities, intentions and plans. Strategic intelligence activities (and the potential they offers to disrupt attacks before they are launched) would be a more productive focus for cyber efforts than some notion of counter-fire or point defense.

The U.S. approach to evidentiary standards also complicates potential responses. The tendency has been to take a legalistic approach with a concomitant high standard of evidence. This high standard is necessary for engagement under both law enforcement and military authorities. Law enforcement action or a military response requires a high degree of certainty in connecting an attack or action to a specific entity. This certainty then allows the authorization of law enforcement or military response, but its absence (and the cyber environment is largely one of ambiguity and uncertainty) produces a kind of strategic indecision that can paralyze response or an active defense based on law enforcement or military authorities.

An alternate approach would be either to use intelligence authorities, which allow for a more flexible response, or to develop doctrine that established that detecting hostile intent and capability was sufficient evidence for some level of counteraction. Successful penetration of an opponent's computer network and the discovery on one of their machines or servers of plans for attacks could be considered sufficient evidence for covert, preventative action even if the evidence did not supply direct attribution for a specific attack.

10. **One tool that the federal government has in its cyber security arsenal is its large buying power. Many of the problems that we have seen in federal government cyber security have been the result of either purchasing insecure software or problems with managed service providers. We've heard some testimony today about not only the need to require more security from our contractors to protect government systems, but also that such reform would better protect critical infrastructure and the general public by encouraging the IT providers to build this security into all their products.**

    a. **How we can get to a point where government is buying more secure products and what challenges we face getting to that point?**
    b. **How do we reform the process so that these products keep up with an ever changing threat?**

The decision to buy more secure products lies entirely with the Executive Branch and OMB has sufficient authority to undertake such an initiative. The Work of the previous administration in creating the "Federal Desktop Core Configuration,"(FDCC) which required venders to sell securely configured products is a useful precedent. The newly developed Consensus Audit Guidelines (CAG) are another useful step in providing a baseline for secure configuration of federal networks. The primary obstacle is the need to define what is required for a more secure product in a timely fashion, but the FDCC and CAG suggest that senior level attention can make this standards development process a priority for management.

11. **I was interested about your comment that the United States has taken better advantage of cyberspace than our competitors have to develop greater economic benefits. Certainly, the growth in the information technology and telecommunications sector has had a profound effect on our economy in recent years.**

    a. **Given that we now know the serious risk and vulnerabilities that also exist in this sector, do you believe that fixing some of these security problems will have the added benefit of helping our economy grow and develop new services?**

b. **To what extent have we been "held back" by these security problems?**

A cynic might say that since people don't care about security, the lack of security has been no impediment to developing new or more efficient services. There may eventually be a time when people begin to refuse to use IT because of fears over security, but we have not yet reached that time. If you wanted a parallel, it would be automobiles. When cars were introduce, people loved them and used them despite the fact they were not safe. Only Federal intervention to require safer tires, seatbelts, safety glass, and other innovations reduced the cost to society of using automobiles. The nation gained much from cars, but it also lost much in avoidable costs. The same it true now for cybersecurity.

It's not so much that the U.S. has been held back as it is that we have inadvertently accelerated our competitors. We pay for research; they share, for free, in the results. We invest in new technology; they get copies of the plans, blueprints, software. Our failure to secure data has allowed competitors (both nations and companies) to close the gap and narrow U.S. technological, military and economic leadership. Poor cybersecurity means that we are subsidizing our competitors.

Answers to Post-Hearing Questions for the Record
Submitted to Alan Paller
From Senator Joseph I. Lieberman

"Cyber Security: Developing a National Security Strategy"
April 28, 2009

Submitted July 13, 2009

1. The National Security Agency (NSA) currently offers the Department of Homeland Security (DHS) technical support for its cyber security activities.

   a. Do you believe that the NSA's domestic responsibilities should expand beyond that supportive role?
   AP: There are two dimensions to the answer to this question. The first focuses on the differences between civilian agencies and military agencies with respect to their relationships with the public and with other agencies and how NSA activities could impact those relationships. The second deals with the location of the expertise needed to protect civilian agencies.
   (1) Military vs. civilian cyber security and the impact of NSA: In general, IT leaders in government feel more confident when NSA assists agencies in determining how to fix their security (an assertion proven at both the Department of Justice and FAA). Where senior people feel confident in the advice, agencies are much more willing to make the changes needed to correct the problems. In general, however, the request for NSA assistance comes only after a major crisis precipitated by a damaging break-in. That doesn't happen across all critical agencies. Therefore the key to taking advantage of NSA's knowledge about configuration and defenses lies in the 20 Critical Controls initiative. Adoption of the NSA-led 20 Critical Controls as the core "common controls" that auditors check for FISMA compliance would be a huge confidence builder and security improver. A bigger issue arises when you go to the next stage - network traffic monitoring. Network traffic monitoring is the only known way to find most infected systems – systems that are capable of changing the "truth" on US government computers. When infected systems "call home" they may leave a tell-tale signature in the network traffic. That signature is changing all the time and the level of analysis needed to stay current is, today, beyond the capacity of DHS. However, if from a policy/privacy perspective, you want to put some distance between NSA and DHS, you could take advantage of some great analysis being done by outside contractor (G2, for example) and ARL (Army Research Lab). DHS could, with the active leadership of Phil Reitinger and Mischel Kwon, develop a powerful NSA-independent consensus to do much better network monitoring. That would be quite useful, especially if the consortium and NSA share findings. The problem this approach might appear to solve, but does not solve, is the one of privacy. To find the persistent presence of attackers in federal systems you must look inside the packets. Whether that is done by NSA or DHS or GSA or the Library of Congress, the risk of misuse of the data is the same. The solution for that problem is simply to put "policemen" in place with sufficient security clearances to make random inspections. The success of that approach is entirely dependent on the privacy credentials of the person in charge of policing. The only person I know who has sufficient trust among the privacy experts is Frank Reeder, the original author of both the Computer Security Act and the Computer Privacy Act, but I expect you would have trouble luring him into such a role.

(2) Where the expertise lies: US leaders would be remiss (negligent?) if they continue to allow unskilled and uninformed people to drive cyber security. Since knowledge of offense (and forensics activities) are the foundation of the information needed for effective defense, and that knowledge is now concentrated almost exclusively in the NSA, the role of the NSA should include continuously updated design and validation of defensive measures. To the extent that agency defenses are informed and driven by guidance from NIST, the advice or standards written by NIST MUST be vetted and prioritized by NSA and US-CERT. Bad security guidance has consistently misled agencies and damaged the nation's ability to defend itself.

b. Why is it important to have open civilian agencies involved in cyber security? Why can't we secure our nation from cyber attack through intelligence and military efforts alone?
AP: Civilian agencies manage highly sensitive information. The Commerce Department's Business and Industry Security division's loss of data on America's most sensitive technologies is one of many, many examples. In addition civilian agencies have a special relation with the public, different from that of military and intelligence agencies: the civilian agencies serve the public directly by delivering government benefits. These relationships demand more open accessibility of civilian computers to the public. Communications; any extended lack of availability or delivery of erroneous information can be catastrophic for public trust. All agencies have a significant role in safely configuring and operating their own systems and that is half the security job. The other half is monitoring traffic. The intelligence agencies can do an excellent job of monitoring traffic for both civilian and military, or DHS can do the job for civilian agencies. As noted in 1(a) above, the real challenges are identical whether NSA or DHS monitors civilian agency traffic or even whether the agency itself monitors it. Bad people can see the information and make inappropriate use of it. It's the watch dogs you choose and the tools they have available that will protect the privacy of the data – not which agency is chosen to monitor traffic.

c. Please describe what you believe to be the ideal relationship between DHS and NSA.
AP: Neither DHS nor NSA actually manage the networks, nor do they secure the systems of government. They are monitoring and advising organizations. Having two such organizations is useful (more eyes looking for problems from varying perspectives). However, the ideal relationship would be a full partnership where they shared what they found and the techniques they use, and where the advice they give to agencies is consistent.

2. The concept of establishing a new White House office to coordinate cyber security policy raises questions about what specific responsibilities the office will assume and the potential lack of congressional oversight.

a. I'm concerned about a lack of transparency and oversight if too much responsibility is moved to the White House – which has been a problem in this area in the past. If a new White House office is created to lead cyber security policy, do you believe it needs to subject to some form of congressional oversight?
AP: You are much more expert than I on this issue. At the risk of showing my ignorance, I'll still try to answer. From what I have seen, it isn't the location of the job that makes oversight effective, it is the relationships between the staffs on the Hill and the staff in the Executive Branch. Building trust, rather than legislating control is the key to effective Congressional oversight.

b. The White House has also recently created the position of Chief Technology Officer, and gave the E-Gov Administrator additional responsibilities as Federal Chief Information Officer. Given that security needs to be considered when making decisions relating to information technology, would the creation of another office create more confusion and make effective management more difficult? How could these offices effectively work together?
AP: It won't be a problem at all if they speak with authority (that comes from deep technical knowledge of attack patterns and defense effectiveness) and with one voice in regards to security.

3. While DHS was given cyber security responsibilities in the Homeland Security Act of 2002 (P.L. 107-296), the arm of DHS entrusted with those responsibilities -- the National Cyber Security Division (NCSD) -- was not given adequate resources or authority to accomplish its mission. In recognition of this gap, NCSD's budget has more than tripled since 2007 under the Comprehensive Cyber Security Initiative (CNCI). However, NCSD still faces many challenges such as attracting qualified staff and lack of authority over any of the entities it's supposed to help secure.

a. What needs to be done to help DHS execute its cyber security mission? Does it need more resources? More authority? A change in organizational structure? More hiring flexibilities? Please explain.
AP: The depth of technical expertise is so low at DHS currently that much of the money is being wasted. Great technical people want to work for leaders who have strong technical skills or have demonstrated the ability to manage technical people well. That is why the selection of Phil Reitinger is so important. But other than Phil and Mischel Kwon (and possibly Admiral Brown, though I don't know whether he has managed great computer people effectively) there doesn't seem to be much technical skill in the management ranks. Managers who are not strong technically are uncomfortable in meetings with (often obnoxious) techies, so they avoid the meetings – often leaving all the work to contractors. That's a perfect formula for failure.

b. Much of the additional funding NCSD has received is funding the expansion of Einstein, an intrusion detection system meant to monitor the networks of federal civilian agencies for intrusions. Is this a good use of funding? If not, where would you recommend investing in order to protect federal networks?
AP: That money seems not yet to have developed a system that gains support. I repeatedly hear from people who have worked with Einstein, "it doesn't work." But I have no first-hand knowledge. Suggestion: Match the capabilities against the system deployed by Tony Pressley and Kerry Long at the ARL – that will give you hard data on how good it is because the ARL system is widely respected by the dozen or so sensitive federal agencies that are getting extraordinary results using it. ARL's system is called Interrogator. It is way ahead of Einstein mainly because it has been operational much longer serving many DD and civilian sites, because it is open to 3rd party analysis technologies; and most importantly because it is being driven by star-quality technical people who have a supportive technical wizard as their boss.. It is a combination of a framework that holds the data and ten or twelve complementary tools that can all operate on the same data simultaneously (on separate servers) and teams of wizards who analyze what is being found. Very impressive comments from people who rely on it. It is not an Army Research Lab project; it is a community-wide project that is housed at ARL.

4. Most federal cyber security efforts to date have been focused on securing government networks. While this is an important endeavor, it's really only a small part of the battle. The vast majority of cyber infrastructure is privately held, yet the impacts of any disruption, destruction, or misuse of these systems are not remotely private. These networks control every aspect of our lives – our electricity, water supply, and bank accounts, to name a few examples. Yet the task of ensuring the security of these systems is challenging since the government does not own them.

    a. Can you please discuss some of the potential impacts of a cyber attack on key critical infrastructure sectors?
    AP: The Wall Street Journal showed that the Chinese had footholds inside US power companies. The Intelligence Community has evidence that the Russians also have footholds inside the utility systems. The CIA reported that remote access to a power system over the Internet caused a multiple city outage. All that leads me to conclude that if we get into a shooting war with either the Chinese or the Russians, the power will go out (and I would guess that communications would stop, as well) in large parts of the United States.

    b. How do we best engage with the private sector to increase cyber security across the private networks?
    AP: Two ways: (1) Have senior intelligence officials invite the CEOs of the relevant companies to a briefing, give them "security classifications for a day," tell them the truth and then (most importantly) tell them what to do and how to measure progress in making those changes. (2) Have the federal government use its procurement power to buy security baked into all the systems it buys. The federal government runs power generation plants, telecommunications, and many other critical infrastructure elements. It can lower the costs and increase the effectiveness of security features very quickly. Federal procurement innovation is the only lever the government has that can bring about rapid and massive improvement.

5. A Center for Strategic and International Study (CSIS) Commission report found that, "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives." Do you believe that some level of regulation is needed to secure cyberspace? If so, in what specific area? Do you have any thoughts on what that regulation would look like?
AP: Electric utilities do not seem willing to press their control systems vendors to deliver more secure technology (possibly because they are worried that would be an admission of vulnerability.) Similarly telecommunications companies are not willing to filter malicious traffic that puts users at risk. The regulation would call for testing, using a series of pre-determined inputs to find how well the industry is protecting its systems. This is equivalent to the tests that the SEC requires public companies to do for their financial systems.

6. One sector of particular concern is the electric sector. Not only does every aspect of economy and way of life rely on electricity, but cyber vulnerabilities with the sector have been well documented. Currently the federal government has no authority to compel basic security practices within the electric sector regardless of how severe a threat we encounter. The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) have both come to Congress supporting additional federal authorities in this area. Do you support legislation providing FERC and

DHS additional authority to ensure the security of the electric sector from cyber attack?
AP: yes, as described in answer to question 5.

7. Cyber criminals are currently stealing hundreds of millions of dollars and often these thefts go undetected by the general population.

   a. Why don't we hear more about these thefts? Who ends up footing the bill when these funds are stolen from an ATM or a bank?
   b. Are financial institutions doing everything they can to prevent these thefts?
   AP (to both questions): When money is taken from bank accounts, the banks foot the bill if the account is personal; business losses are not always covered. Therefore banks have taken extraordinary steps to lessen these attacks. On the other hand, when stolen electronic credit card numbers are used to steal goods or services, the merchant from whom the good sare stolen not only has to foot the bill but also pay the credit card companies a penalty of $0.25 to $1.75 per transaction. Credit card companies may be making as much as $70 million dollars per year from fraudulent transactions. They have not taken the very tough steps they would need to take to radically reduce such losses.

8. The United States is under constant cyber attack. Often times we don't know to a high degree of certainty who is attacking us. This is a new concept in warfare as it's usually fairly easy to trace a physical attack.

   a. Is a cyber attack an act of war?
   AP: Espionage is not, by itself, an act of war. Nations have been doing it for millennia. Otherwise, I am not sure where the line is drawn.
   b. If so, how should we respond – especially if we're not sure who the attacker is?
   AP: Effective defense and rapid recovery are the key to response. We do not have the capacity or surety for a MAD (mutually assured destruction) strategy.

9. One tool that the federal government has in its cyber security arsenal is its large buying power. Many of the problems that we have seen in federal government cyber security have been the result of either purchasing insecure software or problems with managed service providers. We've heard some testimony today about not only the need to require more security from our contractors to protect government systems, but also that such reform would better protect critical infrastructure and the general public by encouraging the IT providers to build this security into all their products.
AP: Federal procurement is the only tool in the US arsenal that can bring about rapid and significant improvement in cybersecurity.
   a. How we can get to a point where government is buying more secure products and what challenges we face getting to that point?
   AP: Four steps:
   (0) Establish a Secure Products and Services Acquisition Board chaired by OMB with key NSA and DHS people in charge (not NIST and GSA – though they can be junior members)
   (1) Convene a series of technical consensus meetings (running as many in parallel as possible) of the people at NSA and DHS (and a few outsiders) who best understand the vulnerabilities in each major technology that the US relies upon. Have that team establish an initial set of configuration settings that provide maximum protection while still enabling mission effectiveness.
   (2) Have one or two major agencies pilot the safe configurations to determine what it takes to make them work effectively in operation.
   (3) Create procurement language that each agency must use (OMB is the only agency that

can do this) to buy the secure configurations baked in and to force system integrators and other vendors who rely on those technologies to use the safe configurations. Sadly, changes in the FAR (Federal Acquisition Regulations) will not work. Federal contractors know that there is not enough money in any contract both to do all the things in the contract specs and to do all the things in the FAR, so they do what is in the specifications of the contract. That has proven to be an effective survival (and profit-making) strategy for the integrators through contracts worth hundreds of billions of dollars over decades. They are not going to change. If you want them to use secure configurations you have to write that (including what specific configurations you are talking about) into each contract. That's why the Secure Products and Services Acquisition Board matters so much. They have the job of keeping that language current and practical, and the stature to make sure contracting officers insist on the presence of the appropriate subset (not some mushy generalization) in each IT services and products contract.

- Steps 1-3 were used to make Windows secure enough to stop spear phishing (the main technique used by the Chinese to penetrate companies and agencies) and most other attacks focusing on Windows.

- The last step was not enforced – mostly because NIST dropped the ball, but in part because Congress was not engaged (may have seemed too technical, but it isn't), so agencies felt they could wait out the change in Administration. Many hope OMB under President Obama will not make them implement FDCC fully. They have implemented some of the FDCC controls, choosing the configuration settings that don't cause any trouble. The problem is that a couple of key controls they are not implementing are the ones that are most critical for stopping known attacks. And it gets more frustrating. OMB under Karen Evans demanded that 100% of the controls be implemented. That was very smart because the Aiur Force proved it could be done. However, without gaining agreement from NSA and the Air Force, the only two agencies that knew what works, NIST added extra controls that that cannot be implemented effectively yet. That put the agencies in an impossible situation – leading to ineffective implementation.

- The most important contracts for improving federal systems are the system integration contracts because without security language baked into the contract, the integrators ask for huge increases in funding whenever they are asked to do security tasks. The 20 Critical Controls developed by CSIS is the key set of requirements that can be asked of system integrators.

b. How do we reform the process so that these products keep up with an ever changing threat?
AP: Because the configurations are risk-based (the configurations reduce known risk), updates to the configurations need to be are risk-based, as well. It turns out that such changes are rare and small. The risks are constantly being identified by industry and NSA and DHS. The Secure Products and Services Acquisition Board can, quarterly, determine which risks need to be reflected in the procurement specs. I believe there will be VERY few changes except when new products (Windows 7, for example) are released. New products are already going through a secure configuration process as they are being designed – because of strong pressure from DoD and strong support from NSA VAO.

Post-Hearing Questions for the Record
Submitted to Tom Kellermann
From Senator Joseph I. Lieberman

1. The National Security Agency (NSA) currently offers the Department of Homeland Security (DHS) technical support for its cyber security activities.

   a. Do you believe that the NSA's domestic responsibilities should expand beyond that supportive role?

   I would suggest that it would be extremely beneficial for the NSA to move actively to expand and strengthen its cyber-security partnership with DHS for a number of reasons – specifically in regards to both the two agencies' strategic relationship related to responding to ongoing cyber-incidents, and in terms of providing DHS cyber-security initiatives with increased access to NSA assets, expertise and intelligence in preparing for potential attacks.

   As currently aligned, DHS does not have sufficient capabilities to deal with either of these organizational mandates around cyber-security. In order to improve its ability to react to attack as quickly and effectively as possible to cyber-attacks, and arm its preventative efforts with all the available information and capabilities necessary to protect critical U.S. government and private sector constituents from future threats, the current NSA-DHS relationship must become a more functional and cooperative partnership.

   The two agencies need to establish more open, direct lines of communication to provide for dynamic contact between their dedicated systems and staff during ongoing cyber-attacks. Stronger ties around information sharing must also be expanded and actively maintained related to incident prevention in order to empower DHS with the most current, comprehensive data available regarding vulnerabilities and attack patterns that can be utilized by potential assailants.

   In general, NSA has significant expertise and robust operational capabilities that can provide enormous value to DHS cyber-security operations, and help those efforts to continue to develop and expand over time. Further, it behooves the NSA to share more information and resources to allow DHS to make smarter decisions and respond faster to benefit its own cyber-security goals and responsibilities.

   Better leveraging the NSA's experience and resources can serve as a bridge in enabling DHS to continue to grow and mature its existing cyber-security operations and architect strategic plans for the future.

   Clearly realizing this entire vision will require hearings, legislation and frank discussions held between the government and privacy/civil liberty groups, and thus will necessitate a longer period of time to come to fruition, but incremental improvements in this partnership can also be achieved in the short term to the benefit of all involved stakeholders.

   b. Why is it important to have open civilian agencies involved in cyber security? Why can't we secure our nation from cyber attack through intelligence and military efforts alone?

Based on the critical nature of IT assets on which the American society has become dependent, most notably those distributed across the grid and infrastructure segments (including the energy, financial, health care, telecommunications and transportation sectors), there is a significant need to involve partners outside of the military and intelligence communities.

In addition to the need to ensure that cyber-security initiatives across all levels of the government retain close familiarity with the critical private-sector IT assets that must be protected from attacks, agencies including the DHS and NSA can learn much from these civilian entities about the nature and implications of today's emerging electronic risks. Specifically, the government can gain crucial insight into those risks inherent to the unique fashion in which many of these heavily-nuanced critical infrastructure assets operate and have been developed from a security standpoint.

For years, the NSA has been viewed as maintaining the most advanced technical expertise and assets, but, as with its relationship with DHS, it must seek to strengthen ties with civilian agencies (such as NERC in the electrical grid space) to ascertain and understand higher levels of situational awareness in regards to matters of national importance related to cyber-security.

The need for these more formal relationships also ties into the demand to expand the Red Team security assessment capabilities of both government and private sector organizations. For, this work will not only improve the ability of those involved to improve their defense-in-depth strategies by identifying vulnerabilities, but also to gain greater insight into larger patterns in IT security risk existent across diverse and distributed infrastructures. Red teaming creates situational awareness.

In this regard, NSA must also move beyond its view of risk to critical infrastructure as primarily related to denial-of-service type events and focus more of its attention on systems infiltration carried out in the name of manipulating and/or corrupting IT assets in the name of advancing their goals against U.S. well-being.

c. Please describe what you believe to be the ideal relationship between DHS and NSA.

Ideally, the relationship between the NSA and DHS in regards to matters of cyber-security response and preparation should emulate the existing liaison in the military realm fostered between the four branches and the U.S. National Guard.

For instance, when the DHS has reached the limitations of its own ability to react to an ongoing cyber-attack and is need of support, its' teams should be able to call upon peers within the NSA to provide additional response and mitigation capabilities.

I would specifically recommend that based on the advanced sophistication of the NSA's Red Team security assessment capabilities and Blue Team remediation expertise, that the agency should make those resources more available not only to DHS but also to the critical infrastructure community (including the energy, financial, health care, telecommunications and transportation segments), under DHS supervision, to help directly address areas of cyber-security risk that have critical importance to national stability.

I would recommend that DHS should lead outreach efforts in the civilian critical infrastructure arena while maintaining a cooperative and functional relationship with the NSA in these matters.

NSA should be prepared to step in to aid DHS cyber-security response efforts whenever cyber-attacks reach a preordained level of critical importance to national security, and should be ready to help establish and maintain partnerships with other important government and private sector constituencies as needed.

All agendas aside, I would think that a close and open relationship wherein the NSA views the DHS as the primary customer and consumer of critical cyber-security capabilities is a fundamental requirement in today's landscape.

I expect that the NSA has been engaged with DHS since the department's inception in sharing IT-based vulnerability and incident information. However, given the NSA's over-arching mission, the need to protect techniques and sources has always been made one of its most prominent organizational characteristics. Consequently, a free flow of real-time information along the lines described previously herein has been severely inhibited. This reality would hopefully subside as a mutual and much needed trust relationship is more firmly established.

2. While DHS was given cyber security responsibilities in the Homeland Security Act of 2002 (P.L. 107-296), the arm of DHS entrusted with those responsibilities -- the National Cyber Security Division (NCSD) -- was not given adequate resources or authority to accomplish its mission. In recognition of this gap, NCSD's budget has more than tripled since 2007 under the Comprehensive Cyber Security Initiative (CNCI). However, NCSD still faces many challenges such as attracting qualified staff and lack of authority over any of the entities it's supposed to help secure.

   a. What needs to be done to help DHS execute its cyber security mission? Does it need more resources? More authority? A change in organizational structure? More hiring flexibilities? Please explain.

      As I noted in my previous testimony before the Committee, it is my overall assessment that while existing DHS efforts have significant value and potential in advancing important matters of cyber-defense, for the most part these initiatives have not been given sufficient financial or operational support to address their all-important mission.

Unfortunately, based on the realities of today's cyber-environment the crawl, walk, run model did not apply to DHS and it has been forced to develop its operations in real time. As a result, while expectations for DHS cyber-security influence have been high, its' capabilities and resources (staff/funds) have been relatively low which has resulted in less than satisfactory success in meeting goals, with little focus committed to developing the organization's capabilities holistically.

As a result of the CNCI, DHS has been able to increase its staffing to a level that begins to approach a minimum baseline. However, I would argue that increased investment in this area is still necessitated.

In addition to the added responsibility for implementing significant parts of the CNCI, DHS continues to manage a significant level of previously ordained cyber-security activities without the benefit of gaining additional resources. It is my opinion that lacking a significant increase in staffing – combined with a more structured organization – DHS will continue to struggle under its existing workload.

Many cyber-security efforts operating under the auspices of DHS also lack sufficient authority to complete their designated missions. A tacit example of this can be found in the NCSD Federal Network Security Branch which is tasked with, among other jobs, hardening U.S. network computing infrastructure against cyber-attack. A specific example of the many organizational challenges faced by the Branch can be found in its oversight of Presidential Directive 23, which addresses governance of Network Operations Center (NOC)/Security Operations Center (SOC) operating standards. While this management function represents a substantial opportunity for the Branch to have a significant impact in improving the capabilities of these installations to help our nation predict and respond to emerging cyber-security issues, it has not been granted the necessary authority to foster the needed defense-in-depth protective IT mechanisms needed to empower these operations.

However, in general, I would recommend that before the issue of broadening the authority of such initiatives operating under DHS is broached, resource levels must first be addressed such that when responsibilities are better outlined involved parties have the needed capabilities to meet their new goals.

In terms of altering organizational structure, as stated earlier, with the added CNCI workload DHS should consider reviewing its current configuration to accommodate both existing and future responsibilities more effectively. However, with the appointment of a Cyber Coordinator on the horizon per White House directive, DHS should ensure that any revised structure would compliment/support the plans and strategies of the Cyber Coordinator as those directives are established.

Related to augmenting hiring flexibility, as I understand, it can currently take up to nine months in order to get qualified staff onboard and cleared to go to work. With that understanding, clearly a more streamlined process would be beneficial. It is almost nonsensical that an organization expected to protect the national information infrastructure would have to wait this long and move this slowly to align resources with its goals. In addition to the laborious hiring process, it's understood that DHS effectively duplicates the clearance process adding months to the hiring/clearance process via the application of the standards process identified as "suitability determination."

U.S. citizens should not tolerate this type of waste of their tax dollars tied to arcane qualifications processes. While the need to establish the credibility and clearance of new staff is critical, this process must be improved for practical purposes. The Office of Cyber Security and Communications should have direct hire authority for all positions, and DHS should accept the OPM clearance process without added qualifications.

b. Much of the additional funding NCSD has received is funding the expansion of Einstein, an intrusion detection system meant to monitor the networks of federal civilian agencies for intrusions. Is this a good use of funding? If not, where would you recommend investing in order to protect federal networks?

While Einstein represents an older form of defensive technology, compared to some other available tools, I do feel this is an acceptable use of funds as despite its shortcomings this project is providing a baseline level of protection.

However, it is also my opinion that monitoring merely for the sake of monitoring provides no immediate value. A bigger issue in regards to Einstein is that it is unknown if DHS has the adequate and qualified analytical resources (people and tools) on hand to support the needed filtering of the vast amount of data produced by this system. It is also unclear if there is a direct and manageable plan that has been established to accomplish this element of Einstein's mission.

In making additional investments, government workforce cyber-security education must be given greater support. Without greater departmental and end user awareness and sensitivity to matters of cyber-security, all the technological protection in the world can easily be compromised by an individual lack of due diligence or exposure to social engineering.

Greater focus must also be placed on ensuring the encryption of electronic data both at rest and "in motion." There must be greater emphasis placed on enforcement and expansion of OMB memo 06-16, issued on June 23, 2006, which requires agencies to encrypt data on all mobile devices and further enlist two factor user authentication. These actions should be extended to encompass data resident on agency desktops, as well as to broaden use of two factor authentication for access to any federal IT system.

Finally, there is a need for NCSD to create expanded Red Team and Blue Team security assessment and remediation capabilities, along with stronger e-forensics programs and dedicated web applications security efforts. The need for more active testing and securing of IT systems to lower risks using all of these processes is crucial. The NCSD would also be well served to expend more of its resources on addressing remote access security measures, including the leadership of development of new authentication technologies.

3. Most federal cyber security efforts to date have been focused on securing government networks. While this is an important endeavor, it's really only a small part of the battle. The vast majority of cyber infrastructure is privately held, yet the impacts of any disruption, destruction, or misuse of these systems are not remotely private. These networks control every aspect of our lives – our electricity, water supply, and bank accounts, to name a few examples. Yet the task of ensuring the security of these systems is challenging since the government does not own them.

    a. Can you please discuss some of the potential impacts of a cyber attack on key critical infrastructure sectors?

    Without overstating the point to the extent that observers might suggest that such depictions could be categorized as overly alarmist, the scope of possible attacks, and the damage that could be affected across the United States via successful cyber-campaigns carried out against critical infrastructure assets must be recognized as incredibly serious, and potentially disastrous.

    From gaining the ability to shut down or manipulate everything from U.S. financial markets to the nation's transportation systems, utilities and communications grids, the list of potential scenarios and various outcomes tied to cyber-attacks against critical infrastructure assets is long, and extremely chilling.

    Looking at the issue within the context of more traditional denial-of-service type attacks that are meant to take crucial infrastructure systems offline, such threats could result in major portions of the nation being thrown into darkness, key financial systems being shut down, widespread loss of access to backbone telecommunications capabilities or interruptions in other vital utilities such as public water services.

    And these are not just theoretical scenarios. As it has been proven with the recent discovery of external infiltrations into large numbers of U.S. government networks and computers, into portions of the U.S. electric grid and into FAA flight control networks, the vulnerabilities allowing for such attacks are widely available and already being exploited by parties located around the globe. The technological capabilities and techniques necessary to carry out these types of DoS campaigns are also highly accessible to constituencies seeking to do so.

However, it is also important to recognize that DoS type attacks are now only the tip of the iceberg in terms of the full range of electronic assaults that could be aimed at U.S. critical infrastructure. As with the efforts of cyber-criminals to infiltrate government and private sector networks and transactional systems in order to steal valuable information for the purpose of committing fraud, attackers are seeking to gain access to infrastructure networks to carry out campaigns through which they can manipulate electronic data and controls to allow them to wreak havoc on American lives.

By gaining the ability to take over command and control of critical networks and alter the integrity of the operations or data running on those systems, versus merely shut them down via DoS, attackers could unleash potential campaigns that may have an even more detrimental effect on the stability of the nation. An example of such behavior might be gaining access to pharmaceutical manufacturing systems to manipulate production and either taint or poison consumer medications and health care products, or to alter the data of electronic financial systems to invoke chaos among U.S. consumers and markets.

b. How do we best engage with the private sector to increase cyber security across the private networks?

The number one priority of the federal sector in better engaging with private entities to address cyber-security challenges on both sides must revolve around establishing more open and dynamic communication among all involved stakeholders. While leaders among both public and private constituencies have long called for this type of close partnership to aid in their respective abilities to thwart greater numbers of cyber-attacks, it would seem that turning those plans into reality has presented a challenge as stakeholders have typically had scant resources or motivation to go about actively pursuing more formalized relations, and thus have not done so with any great success.

I would suggest that parties on both sides must dramatically improve their ability and willingness to share detailed information regarding both ongoing and historic cyber-security experiences and activities if real progress is to be made in allowing government teams to help private sector organizations improve their preparation and situational awareness.

Government agencies and their private sector partners must improve information sharing specifically as it relates to tactical cyber-intelligence, and the government must be willing to offer specialized Red Team and Blue Team capabilities to organizations such as those that control critical infrastructures in order help them rapidly improve their overall security standing in the face of potential attacks.

I would advise that the federal government should also consider the creation of more centralized mechanisms for user authentication to help address the serious issue of unauthorized systems infiltrations left available by insufficient IT access and usage approval controls.

As an example, in Hong Kong the national Post Office has been installed as the certification authority for the regions' central IT authentication program. This is a great model for government-private partnership in the name of making it easier for everyone involved to get on the same page and ensure at least a baseline level of protection for certain types of IT systems and communications.

Currently, U.S. DHS sponsors the Cross Sector Cyber Security Work Group (CSCSWG) and is involved in many other forums aimed at fostering the necessary level of communications between the government and private organizations. However, a recurring theme over the past 6 years has been the inability of DHS to communicate with the private sector operators effectively due to security clearance issues, for, without the prerequisite approvals, DHS is unable to exchange detailed information with their private sector counterparts.

New policies and procedures must be developed within DHS and other government agencies, as well as within private institutions involved in this process to allow for less obstructed communications between the many potential stakeholders with whom it may be necessary to partner closely with around matters of cyber-security

4. A Center for Strategic and International Study (CSIS) Commission report found that, "It is undeniable that an appropriate level of cybersecurity cannot be achieved without regulation, as market forces alone will never provide the level of security necessary to achieve national security objectives." Do you believe that some level of regulation is needed to secure cyberspace? If so, in what specific area? Do you have any thoughts on what that regulation would look like?

Market failure has occurred. There is indeed a need for appropriate legislation to help encourage private sector organizations address their cyber-security challenges, just as it has been necessary to install guidelines in the government sector (such as via FISMA) to push agencies to improve their level of preparation and situational awareness as it relates to cyber-attack.

As it specifically relates to organizations controlling critical infrastructure assets, policy makers should adhere to existing standards that have already proven effective and usable among those attempting to comply with the regulations. At a minimum, these organizations should be required to demonstrate that they have conducted frequent tests of their IT systems vulnerabilities and moved to remediate those problems on a frequent and ongoing basis.

These organizations should also be pushed to require the same level of due diligence from their own business partners and any other third parties that they rely upon for critical services. These requirements should be written directly into their Information Security Service Level Agreements (ISSLAs), and tax credits should be created as an incentive for organizations to adhere to established best practices in protecting their electronic operations.

Market failure by sectors to self regulate – as evidenced by vocal criticism of electrical providers to fall into line around cyber-security resiliency by the bodies assigned to oversee their operational viability, including NERC, or by Congressional criticism of the Payment Card Industry (PCI) Data Security Standard's inability to thwart credit and debit card fraud – demand that the government step in where appropriate to create the necessary mandates that will drive the private sector to better police its own state of cyber-security.

Just as we have existing regulations dictating various aspects of management for our telecommunications, power, water, and transportation systems, the Internet is woven into the economic fabric and our culture to the extent that it must be addressed proactively from a security standpoint. Consequently, we cannot and should not ignore issues that would disrupt our nation's ability to conduct business.

5. One sector of particular concern is the electric sector. Not only does every aspect of economy and way of life rely on electricity, but cyber vulnerabilities with the sector have been well documented. Currently the federal government has no authority to compel basic security practices within the electric sector regardless of how severe a threat we encounter. The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) have both come to Congress supporting additional federal authorities in this area. Do you support legislation providing FERC and DHS additional authority to ensure the security of the electric sector from cyber attack?

As indicated by my previous answers, I would wholeheartedly support the creation of new federal regulations seeking to drive improvement of cyber-security awareness and preparation within the electrical segment. As CIA officials have reported publicly, attackers in foreign nations have already successfully used cyber-attacks carried out on electrical systems, combined with physical attacks, to gain a significant advantage in their hostile efforts.

Organizations controlling elements of the national electrical grid should be mandated to conduct frequent ongoing assessment of their IT vulnerabilities and prove due diligence in trying to fix those problems to the best of their abilities to do so. Red Team and Blue Team exercises must be carried out against these systems on an ongoing basis to ensure that organizations are taking the same view of their assets as outside attackers would and vetting their ability to prevent or allay any available weaknesses.

The federal government must partner more closely with organizations including NERC to understand where infrastructure providers are struggling to secure their assets and align legislation with best practices that allow the complying organizations to directly improve their ability to defend against attacks and improve situational awareness.

Moreover, the most significant issue remains to motivate organizations in this sector to adhere to the highest levels of security practices in specific relation to connecting their private networks with public networks including the Internet.

6. Cyber criminals are currently stealing hundreds of millions of dollars and often these thefts go undetected by the general population.

   a. Why don't we hear more about these thefts? Who ends up footing the bill when these funds are stolen from an ATM or a bank?

   The primary reason that we have not heard more about the ubiquity and severity of these attacks is based on a lack of any perceived benefit on the part of affected parties to make their incidents known publicly, and based on the ability of financial institutions to pass along to costs related to such fraud throughout their customers and supply chains.

   Typically, costs have been passed along to merchants, processors and customers, along with insurance underwriters, in addition to being absorbed by the institutions being attacked themselves.

   However, there have been fairly recent changes within the banking and payment processing industries that have led to these types of attacks becoming so much more ubiquitous and financially damaging that organizations have reached a point where they must ask for help, including seeking greater support from government agencies and industry regulators.

   The leading catalyst to this end has been the move by financial institutions to accelerate the manner in which they process and fulfill electronic payments and transactions, namely via the adoption of Straight Through Processing (STP).

   Whereas attackers have traditionally focused most of their efforts on stealing consumers' personally identifiable information for the purpose of committing identity theft and/or fraud, many assailants have now begun taking advantage of these institutions' newer processes whereby funds are awarded at the time of the transaction, versus some time afterwards, to steal funds and immediately work to begin laundering those assets. Along with the ability to use online payment services such as Web Money and e-Gold to rapidly transfer funds outside of the traditional financial sector and convey those monies into tangible assets that they make off with immediately, attackers are effectively gaming these electronic banking systems to enrich themselves with little risk of being caught by law enforcement officials.

   At the heart of the issue remains the problem that many banks and financial services institutions lack sufficient security controls for their networks or their customers, and fail to require their business partners to maintain higher standards of security for their own operations – therein enabling attacks that seek to transport through those systems into those of the banks themselves.

Because of these phenomena, hackers have realized over the last several years that they can now steal money out of payment systems with banks having almost no ability to unwind payments based on STP parameters. This has led to a significant increase in incidents overall, including large value wire fraud, with many banks now trying to transfer security responsibility to account holders for not sufficiently protecting their own computing systems, which is, in my opinion, a travesty. According to FINCEN--Wire transfer fraud appears on the rise. Since April 1996, 53,590 Suspicious Activity Reports (SARs) have been filed identifying wire transfer fraud. *Disturbingly, Nearly half of those filings came in the past two years.*

b. Are financial institutions doing everything they can to prevent these thefts?

The majority of institutions are not doing enough, though some have become more proactive in trying to assess and address related risks. The most significant gaps remain in the financial services sector around matters of electronic customer authentication.

Having failed or fallen short in efforts such as providing customers with two-factor authentication credentials, and neglected to perform necessary regular penetration testing exercises to understand and fix their most pressing IT vulnerabilities, specifically in validating the security of their online banking systems, thus most financial institutions remain woefully vulnerable to staged cyber attacks. Finally, many or these organizations lack sufficient systems logging and forensics capabilities to understand the criminal incidents which have impacted them.

One simple action would be to require all financial organizations to offer and provide two-factor authentication to their customers, however incentives must also be created for encouraging more customers to utilize those tools. This may require a one-time or reoccurring expense on the part of the financial organizations, but I feel that many customers would understand the value and take advantage of the added security tools.

7. The United States is under constant cyber attack. Often times we don't know to a high degree of certainty who is attacking us. This is a new concept in warfare as it's usually fairly easy to trace a physical attack.

    a. Is a cyber attack an act of war?

1) This is a question that begs situational interpretation, but the answer in some cases is unquestionably yes. Attacks, in particular those that could be traced to any specific nation state or terrorist organization, that seek to destroy or undermine the ability of United States electronic infrastructure to function properly, such as attacks that seek to cripple or corrupt financial or transportation systems to negatively affect the ability of Americans to go about their lives, must be considered through this lens

To further clarify this issue, leadership within the NSC, DHS and DoD should create operational plans defining what types of cyber-attacks would be considered an act of war and what actions should be taken in response. There should be clear boundaries or actions that when crossed and detected may constitute an act of war and the necessary policies, plans, and processes must be in place to address such situations.
Some examples of cyber warfare are:

1. Attacking the central depository for Wall Street.

2. A successful DoS against the electric grid.

3. A cyber attack on a pharmaceutical manufacturer which poisons Americans who consume the product.

4. A cyber attack on the air-traffic control system which creates a catastrophic plane crash.

b. If so, how should we respond – especially if we're not sure who the attacker is?

Attribution remains a serious problem, stemming from a lack of sufficient incidence response and e-forensics capabilities and the reality that many times attacks are launched from compromised computers e.g. botnets whose owners have no knowledge of how their assets are being misused. This is also driven by a lack of due diligence around IT vulnerability management and Red Team testing of those systems to find and address available weaknesses.

There also remain fundamental issues with organizations' retention of computing logs, along with a general inability for the government to more strictly police ISP customers to better deduce where attacks are coming from.

That said, in those cases where aggressive cyber-attacks are clearly being generated from a specific corner of the globe, political and even military actions must be threatened and even applied in order to have an impact in stemming this behavior, just as in all other areas of international policy. However, one should never take any offensive action without fully understanding the source as well as being prepared to address any consequences that may entail following any responsive action(s).

The United States cannot create Fortress America in cyber-space, we must seek the support and partnership of nations, worldwide and international bodies such as the United Nations and G8 to contain and address cyber-attack outbreaks. We must also partner with the developing world to create incentives for enforcing cyber-crime laws and to undermine the existing "Robin Hood" mentality within certain regions where using electronic means to steal from Americans is ignored by local law enforcement and even celebrated based on the notion that this activity somehow levels the socio-economic playing field.

Thank you for the opportunity to submit responses to these questions. I am honored to contribute. I appreciate your consideration and service to our great nation.

Sincerely,

Tom Kellermann

Prepared Statement of Chairman Joseph Lieberman

"Cyber Attacks: Protecting Industry Against Growing Threats"

Homeland Security and Governmental Affairs Committee
September 14, 2009

Good morning. There's an old saying familiar that: "No good deed goes unpunished." The modern technological corollary of that could be: "No good invention goes unexploited for bad purposes."

And so it is in the world of cyberspace – as enemies and criminals have used it increasingly to attack business and our federal, state, local governments.

It was only forty years ago that the first two computers were connected into what is now the Internet. Now nearly the entire world is on line. The Internet has led to a wonderful revolution in commerce, communications, entertainment and finance that has added greater efficiency, convenience, and pleasure to our enterprises.

But, again, it seems: "No good invention goes unexploited for bad purposes."

And that successful computer experiment 40 years ago that gave us this interconnected world has also given us a global wave of cyber crime that threatens both our national security and the integrity of our economic security.

In a hearing last April, this Committee examined in detail the threats to national security brought on by terrorists, nation states, common hackers, and cyber criminals.

We learned, for example, that computers containing information on the joint-strike fighter and our electrical grid have been compromised, possibly giving our enemies information that could make our fighter planes more vulnerable and, at worst, plunge our cities into darkness.

Today, we will focus on a new wave of cybercrime that is hitting businesses of all sizes across our country and ask the question: "What can be done by the public and private sectors to make commercial cyberspace secure, especially for organizations that can't afford to have large IT staffs on the job 24/7?"

We will hear from two witnesses from the private sector who will describe what real cybercrime is and what the private sector is doing about it and two witnesses from the federal government.

The latest targets of cybercrime are small- and medium-sized businesses.

In one particular example, cyber criminals operating out of Eastern Europe stole millions of dollars from businesses and local governments by first sending a seemingly innocuous e-mail to an unsuspecting company comptroller or treasurer. The message contained either a virus or an Internet link that installs a tiny piece of computer code designed to steal passwords.

Using those passwords to gain entry to accounts, the crooks then patiently siphon off amounts less than the $10,000 that would trigger a bank report under federal anti-money laundering requirements. Their methods are so sophisticated that the traffic seems to be coming from an authorized computer – which could be a legitimate computer that has been commandeered – so the bank doesn't know anything is amiss.

The money is then transferred to "money mules" – people recruited to set up bank accounts the stolen money can be transferred to and who then forward the money to the cyber-criminals.

Some of these people may not even be aware they are taking part in a crime. They are often recruited to become "local agents" handling cash transfers for what they believe to be a legitimate company.

The cyber gangs find these people over Internet job boards by advertising the chance to "make money from home" or by contacting people directly who have posted resumes on a legitimate job service.

Once the money shows up in the accounts the mules have set up, they are given instructions on how to wire it to other accounts controlled by cyber criminals.

Cyber criminals, using this basic system have already stolen a lot of money: $700,000 from a school district near Pittsburgh; $100,000 from an electronics-testing firm in Baton Rouge, La.; and $1.2 million from a Texas manufacturer.

These, of course, are only a few examples of what can only be described as a cybercrime wave.

In 2007, TJX Corporation – the parent company of T.J. Maxx and Marshall's – experienced a breach in its wireless networks during which up to 94 million credit and debit card numbers were put at risk of being used illegally.

In 2008, Heartland Payment Systems – whose CEO is testifying before us today – was targeted by hackers in an attack that compromised at least 130 million credit card accounts.

These are just the large intrusions we know about – a lot of these cyber attacks go undetected or unreported because the victims are too frightened to report them – because of security reasons, or they've been threatened, or they don't want it known that it happened.

This can't go on. Forty years ago, the Internet was a tiny island of interconnected university computers that, while vast in potential, was still just an interesting academic experiment.

Today the Internet is a global asset – a new strategic high ground we call "cyberspace" – that we must secure just as any military commander would seize and control the high ground of a battlefield.

But securing cyberspace is much more complicated to do since the Internet is, by nature, a limitless place and security cannot be achieved by the government or private sector alone or by either or both easily.

A public-private partnership to defend the integrity of cyberspace is essential. Together, business, government, law enforcement throughout the world must come together to deter these attacks and bring these criminals to justice.

Our Committee is working on legislation that will help make this so, specifically to further define and strengthen the role of the Department of Homeland Security in protecting all of us in cyberspace.

I hope that this hearing will help educate the Committee on how best to protect the private sector in that legislation.

Opening Statement of Senator Susan M. Collins

Cyber Attacks: Protecting Industry Against Growing Threats

Committee on Homeland Security and Governmental Affairs
September 14, 2009

We are living in a wondrous new age of global information, an era that is being shaped by digital technology, consumer demand, and amazing innovation.

It truly is a remarkable time. Today, without thinking much about it, we send pictures, words and video over the Web in a matter of seconds. We have immediate, 24/7 access to each other, texting and talking over affordable wireless devices. Technology is transforming our culture, our economy, and our world.

While we enjoy its many benefits and most people cannot imagine life without computer technology, we also must be aware of the risks and dangers posed by this new world.

For every communications advance, there also is the risk that the technology will be misused and exploited. Indeed, experts estimate that cyber crime has cost our national economy nearly 8 billion dollars in losses.

Protecting our cyberspace has become critically important. In the past 18 months, this Committee has held three hearings on the topic of cybersecurity.

Each time, we confronted a new line of cyber crime or cyber attacks. Newspaper headlines paint a troubling picture of the state of information technology security in this country.

- This past Friday, computer hacker Albert Gonzalez pleaded guilty to charges stemming from the theft of tens of millions of credit and debit card numbers from the computers of several major retailers, including Barnes & Noble.

  According to authorities, this may not have been his only major cyber crime. In August, he was indicted for his alleged involvement in the largest credit and debit card data breach ever in the United States. Data relating to more than 130 million credit and debit cards were stolen from a number of corporations, including Hannaford Brothers – a Maine-based supermarket chain – and Heartland Payment Systems, whose CEO is testifying today.

- In July, the United States and South Korea endured a sizeable denial of service attack against both government and privately owned systems. The attack – launched by an unknown attacker – used a massive "bot-net" of hijacked computers to disrupt six federal agencies, the Washington Post, NASDAQ, and other targets.

- Most recently, there has been a significant increase in organized "cyber gangs" stealing money from small and mid-size companies. The Financial Crimes Enforcement Network reports that wire-transfer fraud rose 58 percent in 2008, with businesses generally forced to swallow substantial losses that they can ill-afford in the current economy.

These incidents – coupled with the attacks and crimes that we have discussed in past hearings – should prompt the federal government to get organized and make cybersecurity a higher priority. Thankfully, there has not yet been a "cyber 9/11," but information technology vulnerabilities are regularly exploited to steal billions of dollars, disrupt government and business operations, and engage in acts of espionage, including theft of business and personal data. These incidents can be devastating to our national security, erode our economic foundations, and ruin personal lives.

We are awash in recommendations on how to better secure our information infrastructure. The Center for Strategic and International Studies, the 60-Day White House Cyberspace Policy Review, and numerous academics and industry stakeholders have suggested ways to improve cybersecurity. As these latest incidents underscore, however, the time has come to move on from simply planning to action.

Comprehensive cybersecurity legislation must be a high priority for this Congress. The Department of Homeland Security is designated the lead agency for cybersecurity, and we must ensure that it has the authorities necessary to effectively carry out this mission. These authorities must include:

- Sharing critical information on threats and vulnerabilities with the private sector since 85% of critical infrastructure is privately owned;

- Encouraging the adoption of best practices and standards across the government, throughout our nation's critical infrastructure, and in our nation's business community;

- Generating a strategy that deters terrorists and hostile nation-states from executing cyber attacks that could potentially devastate our critical infrastructure; and,

- Establishing standards and performance metrics that can guide government procurement and thereby encourage manufacturers to incorporate better security into their products for the benefit of both the government and the private sector.

I look forward to discussing how we can build a strong public-private partnership to ensure the security of this vital engine of our economy.

Statement of Robert Carr, Chairman and CEO Heartland Payment Systems, Before the Senate Committee on Homeland Security and Government Affairs

September 14, 2009

Good morning Chairman Lieberman, Ranking Member Collins, and Members of the Committee. My name is Robert O. Carr, and I am the Chairman and Chief Executive Officer of Heartland Payment Systems, Inc.

Let me begin by thanking the Committee for this opportunity to appear today to share our lessons learned and the steps we have taken and what more can and should be done to better protect our customers and the public from criminal hackers.

Our primary business is to provide bank card payment processing services to merchants. This involves facilitating the exchange of information and funds between merchants and cardholders' issuing financial institutions, providing end-to-end electronic payment processing services to merchants, including clearing and settlement, merchant accounting, and support and risk management.

When a consumer's card is swiped at one of our merchants, we forward the authorization request through Visa or MasterCard to the issuing bank, and then send their approval back to the merchant, allowing the purchase to be

made. In the following days we will receive payment from the issuer and pass it on to the merchant, and provide statements and accounting to the merchant. It is important to note that in the course of our payment processing business we do not receive cardholder social security numbers, addresses or unencrypted PIN data.

We were founded in 1997, and have since grown to represent over 3,100 employees, with over 1,200 W-2 salespeople across the nation. As of December 31, 2008, we provided our bank card payment processing services to approximately 230,000 merchants. Our total bank card processing volume for 2008 was almost $67 billion.

On January 20, 2009, we announced the discovery of a criminal breach of our payment systems environment. This attack involved malicious software that appears to have allowed criminal access to in-transit payment card data while it was being processed by Heartland during the transaction authorization process. This data is not required to be encrypted while in transit under current payment card industry guidelines.

We were pleased to hear the recent news about law enforcement's efforts to investigate and prosecute the individuals who make up the criminal syndicate that law enforcement believes is responsible for the Heartland breach and others like it. Albert Gonzalez, the alleged mastermind of attacks on TJX and other retailers including Barnes Noble, Office Max, and Dave & Buster, has pled guilty to charges in a 19-count indictment that includes conspiracy, wire fraud, and aggravated identity theft charges. Mr. Gonzalez is also accused of having hacked into our system, as well as that of Hannaford Brothers, ATMs stationed in 7-11s and two other national retailers. It is reported that he was part of a team with eastern European criminals who have attacked a variety of U.S. companies.

We appreciate the efforts federal law enforcement are making to help stop these attacks and to bring these criminals to justice.

This has been a difficult experience for me and the company. We have taken a financial charge of approximately $32 million just in the first six months of this year on forensics, legal work, and other related efforts. Unfortunately, the company is involved in inquiries, investigations and litigation, so I cannot address in more detail the specifics of the intrusion. But I now know that this industry needs to, and can, do more to be better protected against the ever more sophisticated methods used by these cyber criminals, and I want to provide this Committee with some additional information about what Heartland is working on to try and prevent such intrusions in the future.

Let me note two key areas where Heartland is hard at work to address industry deficiencies.

First, industry and government can be better coordinated. The Financial Services Information Sharing and Analysis Center or FS-ISAC has been a great resource to a broad range of financial services companies facing this

threat but I realized that we could benefit from greater focus on the payment processing industry. In order to address the needs of payment processors, we recently formed, within the FS-ISAC, the Payments Processing Information Sharing Council (PPISC), a forum for sharing information about fraud, threats, vulnerabilities and risk mitigation practices.

At the PPISC, I shared with the payment industry members the malware which we discovered had been used to victimize Heartland. I did this once I learned that criminals were using this malware to attack our industry. I believe that by sharing this with others, including our industry competitors, we can better respond to very organized attackers.

Second, as reflected in the indictments of Mr. Gonzalez, a modus operandi frequently used by these attackers is to attempt to steal payment card data while it is being transferred in the clear - meaning it was not encrypted at the time. It is clear to me that we can address this vulnerability, and our internal technology team is continuing the development of a possible solution we call E3 - end-to-end encryption. I believe it is critical we implement this new technology, not just at Heartland, but industry-wide. We at Heartland believe we are taking the necessary steps to do so.

Heartland is working to deploy E3 to render data unreadable to outsiders from the point of card swipe. We plan to use special point-of-sale terminals, with Tamper Resistant Security Modules, TRSMs, to protect cryptographic secrets. We also plan to use special tools in

our processing network, Hardware Security Modules, to protect the cryptography associated with the card data.

Our goal is to completely remove payment account numbers of credit and debit cards and magnetic stripe data such as expiration date, service codes, and other data, so that it is never accessible in a usable format in the merchant and processor systems.

We are taking the necessary steps to implement this E3 solution, and I want to let the Committee know where our efforts stand.

1. **We are working with various suppliers on the technology to make E3 a reality and more ubiquitous. We are hopeful that these efforts will minimize the costs to merchants while not inconveniencing cardholders and yield a payment processing system that is more secure. We are seeking partners who will not use encryption as an opportunity to profit at our expense or that of our merchant customers.**

2. **We believe this potential solution needs to be implemented on an industry-wide basis. We have been working with the Accredited Standards Committee X9 (ASC-X9), to seek adoption of a new standard to protect card holder data in the electronic payments industry so all users can benefit from it. Ultimately, the Payment Card**

Industry Security Council must approve this standard and we are hopeful that it will do so soon.

3. **Once the standards are established, we will need the card brands and other financial institutions to cooperate and to be willing to implement on their side the encryption system our merchants are willing to use. We have been meeting with the card brands and the issuers and we hope we will be able to make progress on adoption by the card brands. However, without the cooperation of all of the card brands, the encrypted data would have to be decrypted --and thereby rendered less secure, prior to transmission to the card brands and their issuing banks. I am hopeful that each of the card brands will ultimately accept encrypted transactions from Heartland and other processors.**

We are working on these solutions, both technological and cooperative, because I don't want any one else in our industry or our customers or their customers - the consumers - to fall victim to cyber criminals. The attacks we face in this country potentially can have substantial consequences but we can learn from our experience and, while we cannot eliminate the risk, we can make cyber theft more difficult. I look forward to continuing to work to beat these criminals and appreciate your help as we continue this battle.

I welcome any questions Members of the Committee may have about my testimony today.

***** As the CEO of a publicly traded company I note that several of the statements in this testimony and that may be made in response to questions relate to events that are expected to occur in the future. The actual outcome of the future events I discuss is subject to risks and therefore, it is possible that the actual outcome of these future events may turn out to be different than the projected outcomes described.**

Testimony of

William B. Nelson

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States Senate

Committee on

Homeland Security and Governmental Affairs

September 14, 2009

FS-ISAC BACKGROUND

Chairman Lieberman, Ranking Member Collins, and members of the committee, my name is William B. Nelson, I am President and CEO of the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the U.S. Senate Homeland Security and Government Affairs Committee on the important issue of Cyber Crime and its impact to the financial services industry.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,100 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 40 trade associations representing the majority of the US financial services sector.

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security, Federal Reserve, United States Secret Service, Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and state and local governments.

With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and by agreement is identified as the operational arm of, the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also work closely with other industry groups and trade associations including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Financial Services Technology Consortium (FSTC) and the BITS division of the Financial Services Roundtable.

The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the originator and shared for the good of the sector, the membership and the nation. A complete list of FS-ISAC information sharing services and activities include:

- Provision of timely, relevant and actionable cyber & physical email alerts from various sources distributed through the 24x7x365 FS-ISAC Security Operations Center (SOC)
- Preparing cyber security briefings and white papers

- Engagement with private security companies including but not limited to, Verisign/iDefense, Symantec, McAfee and Secure Works to identify threat information of relevance to the membership and the sector.
- Preparing risk mitigation best practices and toolkits
- Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee that provide in-depth analyses of risks to the sector, provide technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics.
- Hosting document repositories for members to share information and documentation with other members
- An anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner
- Operation of email list servers supporting attributable information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, a broader Threat Intelligence information sharing list and a new list to support the Payment Processors Information Sharing Council (PPISC) which functions as a Council of the FS-ISAC
- Anonymous surveys that allow members to request anonymized information regarding security best practices at other organizations
- Conducting bi-weekly threat information sharing calls for members to discuss the latest threats, vulnerabilities and incidents and allow guest speakers on risk related subjects
- Providing emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS)

- Conducting emergency conference calls to share information with the membership and solicit input and collaboration.
- Developing and testing crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies.
- Conducting semi-annual Member Meetings and conferences
- Conducting online presentations and regional outreach programs to educate small to medium sized regional financial services firms on threats, risks and best practices.

A key factor in all of these activities is trust. The FS-ISAC works to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations particularly the law enforcement and intelligence communities.

PUBLIC/PRIVATE SECTOR RESPONSE TO THE CYBER CRIME ISSUE

The FS-ISAC is well aware through its information sharing arrangements with both public and private sector organizations that criminal threats are targeting US financial institutions, businesses and consumers. However, discussions with a number of larger financial institutions reveals that cyber crime losses currently only account for a small percentage of the overall fraud loss encountered by these institutions. That is not to say that trend in online fraud is not increasing, just that when taken in the overall fraud context of an institution, the number of incidents and consequent losses appear lower than losses from other fraudulent activity.

The FS-ISAC and its members do recognize the online criminal threat both to the affected institutions and to consumer confidence posed by these criminal activities and we are taking steps to address areas of concern.

Law enforcement and a number of government agencies have taken a lead role working with the FS-ISAC, its member organizations, payments processors, and the financial services sector as a whole to combat these types of attacks. An example of a successful instance of government/financial services sector information sharing occurred on August 24, 2009, when the Federal Bureau of Investigation (FBI), the FS-ISAC and National Automated Clearing House Association (NACHA is the rule-making body for the automated clearing house network) released a joint bulletin concerning account takeover activities targeting business and corporate customers. The bulletin described the methods and tools employed in recent fraud activities perpetrated against small to medium-size businesses that had been reported to the FBI. The objective of the information sharing and ultimately the bulletin was to employ FS-ISAC and NACHA subject matter expertise applied to the FBI case information to identify detailed threat detection and risk mitigation strategies for financial institutions and their business customers, whilst preserving the integrity of the FBI's ongoing investigations. The bulletin was distributed through the FS-ISAC to its over 4,100 members which includes over 40 member associations such as NACHA, the American Bankers Association, Independent Community Bankers Association, amongst others.

The risk mitigation tactics that are outlined in the joint FBI/FS-ISAC/NACHA bulletin include information security best practices that are consistent with the Federal Financial Institutions Examination Council's (FFIEC's) Guidance, *Authentication in an Internet Banking Environment*. However, since regulatory agencies have not focused on account takeover issues specific to this type of attack, the FS-ISAC and NACHA developed a comprehensive list of recommendations to financial institutions to educate their business customers on the need to use online banking services in a secure manner. (Please note that details of those recommendations are not provided in this testimony due to concerns that this information could be disclosed publicly and used by the criminals to develop new methods and tools to defeat those controls.) As a result of this bulletin, financial services firms and their business and corporate customers have become more aware of some of the online risks facing them, how to detect malicious and criminal activities, and effective practices to mitigate those risks.

The FS-ISAC provides the 24x7x365 platform for its members to share information between themselves, with the government and law enforcement, and with other sectors. The FS-ISAC participates in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and provides support for FSSCC exercises such as CyberFIRE. The FS-ISAC is undertaking a major effort on its own to conduct a national Cyber Payment Attack Exercise in the first quarter, 2010. The plans include a variety of simulated attacks that will test the financial services industry's ability to respond and react to different types of cyber attacks. The exercise will also provide a forum to raise awareness regarding best practices and remediation steps to minimize the risk to the financial services firms and their customers from these various types of attacks. Participation in the exercise will not be limited to FS-ISAC members alone. In fact, the entire financial services industry will be invited to participate along with the business community and retailers.

From a law enforcement perspective, recent progress has been made against some cyber crime activities. Indictments have been handed down against several individuals accused with responsibility for the attacks against Hannaford Brothers supermarkets, 7-Eleven and Heartland Payments System. This is an important step by law enforcement to stem the tide of rising cyber attacks by going after the criminal masterminds behind them. Arrests have been made in these particular cases but some of the cyber criminals indicted operate in other countries, mostly in Eastern Europe, and they remain at-large. An area where our Federal Government could help is to force better cooperation from those countries' governments that fail to cooperate in these types of cyber crime investigations and prosecutions.

Cyber Security Collaborative Efforts by the Financial Services Industry

The FS-ISAC is a member of the Financial Services Sector Coordinating Council (FSSCC) and is viewed as the FSSCC's operating arm. Through the FSSCC, the private sector financial service industry collaborates with Financial and Banking Infrastructure Information Committee (FBIIC) which consists of the key financial services industry regulators involved in critical infrastructure protection such as the U.S. Treasury, the Federal Reserve, the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and others. FSSCC and FBIIC members meet regularly and participate in classified briefings from law enforcement and the intelligence community where important vulnerability and threat information is exchanged.

Financial regulators are actively involved in developing regulations and supervisory guidance and in conducting focused examinations of information security, vendor management and business continuity controls at financial institutions and major service providers. There are nearly a dozen booklets covering these key cyber security and business continuity issues in the FFIEC handbook.

The FS-ISAC also works closely with other key financial services industry groups to protect the industry and its customers against cyber threats. A few of these organizations include the American Bankers Association (ABA), the Independent Community Bankers Association (ICBA), BITS- the technology and operations division of the Financial Services Roundtable, the Financial Services Technology Consortium (FSTC), and many others. The following is a partial list of activities that the financial services sector has undertaken to improve the industry's response to online criminal activities:

- The ABA and ICBA have been instrumental in increasing the membership levels and reach of the FS-ISAC to over 4,100 members today. And through the FS-ISAC's 40 association members, the reach of the FS-ISAC is nearly universal to every regulated financial institution in the U.S., regardless of its size.

- BITS and the Financial Services Roundtable have launched the Identity Theft Assistance Center (ITAC), a nonprofit coalition of financial services companies united to protect their customers from identity theft. ITAC's victim assistance service – which has helped more than 55,000 consumers recover from identity theft – is available at no cost to the millions of consumers who have an account at an ITAC member company.

- The FSTC has led a number of important projects to improve the security of member financial institutions and their customers. This includes a joint project with BITS on a secure web browsing initiative aimed at helping prevent some forms of these attacks. The FSTC, BITS, ABA, and FS-ISAC have also engaged the Internet Corporation for Assigned Names and Numbers (ICANN) on improving the security and stability of the Internet.

- Recently, the ABA, FS-ISAC, BITS and FSTC have worked with the Federal government's General Services Administration, Internal Revenue Service, and the Social Security Administration to develop better ID assurance for online e-government applications. The goal of this effort is to leverage the "Know Your Customer" requirements that banks, credit unions and other financial services firms employ for ID proofing and turn that into higher levels of assurance for access to online government applications. The project is in the proposal phase at present and still requires a funding commitment and more definition around the business model and system architecture. However, it is a prime example of how public/private sector cooperation is beginning to progress in the important area of online ID assurance.

Additional Steps That Industry and the Federal Government Can Take Together

Rather than outline a series of recommendations that the financial services industry should take independently and a separate set of recommendations that the Federal Government should address, I chose to develop a consolidated approach for both. I think this better illustrates the need and commitment that we must have for public/private sector cooperation in protecting the industry and the nation's citizens from the growing threat of cyber crime.

1. Improve Cyber Crime law enforcement
   a. There needs to be better and more domestic and international collaboration regarding investigations and prosecutions given the origins of a significant portion of cyber crime. Countries that have not adopted the Council of Europe's Convention on Cybercrime should be encouraged to do so. The Convention is an international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes.
   b. Sufficient funding is needed for cyber crime investigations and forensics. Currently, private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers so the cumulative dollar value of the crime committed may be many times the amount of one particular loss.
   c. Law enforcement must be more responsive to cyber crimes reported by financial services firms. There needs to be improved communications at a local level between financial services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action will be taken.

2. Improve Financial Institution Information Security Programs

Regulators and industry need to have a flexible and dynamic approach to cyber security so that individual financial institutions can continue to improve information security programs based on their size, scope of activities, and structure. This builds on the foundation embodied in the Gramm-Leach-Bliley Act framework and opposes prescriptive, one size fits all or technology-specific approaches.

3. Stronger Authentication and Encryption

Financial services firms, processors and regulators need to encourage smart use of encryption and stronger authentication through regulatory safe harbors bearing in mind that encryption and authentication solutions must achieve the appropriate balance between security, risk and usability.

4. Improve public/private Sector collaboration

Expanded information sharing between Government agencies and the financial services industry is one of the FS-ISAC's primary goals. There needs to be greater private sector access to threat and intelligence from Federal intelligence and law enforcement agencies, administered in a manner that can provide broader protection without providing undue market advantage to a select group or that would compromise ongoing investigations. Specific recommendations include:

a. Provide financial institutions, networks and processors with timely, "relevant and actionable" information on threats, vulnerabilities, and exploits.

b. Provide the financial services industry with analysis of trends using existing data reporting requirements (e.g., Financial Crimes Enforcement Network's data of Suspicious Activity Reports which includes computer crimes)

c. Support ISACs such as the FS-ISAC and sector coordinating councils such as the Financial Services Sector Coordinating Council (FSSCC) for the private sector and the Financial and Banking Information Infrastructure Committee (FBIIC) for the public sector, and support their joint initiatives.

d. Compile and share data on payment system fraud and security trends

e. Fund top R&D priorities, such as enrollment and identity credential management and data centric protection strategies (see https://www.fsscc.org/fsscc/reports/2008/RD_Agenda-FINAL.pdf)

5. Improve the Internet Infrastructure

Use federal procurement power to improve the security of software, hardware and services that support the Internet business infrastructure and applications (i.e., enhanced technology that is implementable and cost appropriate for the market.)

6. Education

More public/private sector collaboration is needed to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices. One example of such an effort has been undertaken by the National Cyber Security Alliance in promoting a "Stay Safe Online" campaign as part of the October Cyber Security Awareness month. Some financial institutions have done a good job of educating their customers re:

phishing and other social engineering attacks with information on their websites, mailers and in their bank lobbies regarding safe and secure online banking practices. One concept that has been discussed by some banks and banking associations in Virginia and West Virginia is to develop a national anti-phishing campaign with a "No Phishing" logo to increase public awareness about this threat. However, more resources are needed to effectively take that concept and roll it out at a national level.

Thank you again for this opportunity to present this testimony and I look forward to your questions.

Statement of Mr. Michael P. Merritt

Assistant Director
Office of Investigations
U. S. Secret Service

Before the Senate Homeland Security and Governmental Affairs Committee

U.S. Senate

September 14, 2009

Good morning, Chairman Lieberman, Ranking Member Collins and distinguished members of the Committee. Thank you for the opportunity to address this Committee on the subject of cyber and computer-related crimes and the role of the U.S. Secret Service (Secret Service) in cyber investigations.

While the Secret Service is perhaps best known for protecting our nation's leaders, we were established in 1865 to investigate and prevent the counterfeiting of United States currency. As the original guardian of the nation's financial payment system, the Secret Service has a long history of protecting American consumers, industries, and financial institutions from fraud. Congress continues to recognize the Secret Service's 144 years of investigative expertise in financial crimes and over the last two decades has expanded our statutory authorities to include access device fraud (18 USC §1029), which includes credit and debit card fraud. Congress has also given the Secret Service concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344). We take our mission to combat these crimes seriously and as a result, the Secret Service is recognized worldwide for our investigative expertise and innovative approaches to detecting, investigating, and preventing financial crimes.

Trends in Cyber and Computer-Related Crimes

In recent years, the Secret Service has observed a significant increase in the quality, quantity, and complexity of cyber-cases in which perpetrators target financial institutions in the United States. The combination of the information revolution and the effects of globalization have driven the evolution of the Secret Service's investigative mission. The advent of technology and the Internet created a new transnational "cyber-criminal," and as a result the Secret Service has observed a marked increase in cyber and computer-related crimes targeting private industry and other critical infrastructures. For example, trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the American economy. As large companies have adopted more sophisticated protections against cyber-crime, criminals have adapted as well by increasing their attacks against small and medium-sized businesses, banks, and data processors. Unfortunately, many smaller businesses do not have the resources to adopt and continuously upgrade the sophisticated protections needed to safeguard data from being compromised.

The Secret Service is particularly concerned about cases involving network intrusions of businesses that result in the compromise of credit and debit card numbers and all related personal information. A considerable portion of this type of electronic theft appears to be attributable to organized cyber-groups, many of them based abroad, which pursue both the intrusions and the subsequent exploitation of the stolen data. Stolen credit card information is often trafficked in units that include more than just the card number and expiration date. These "full-info cards" include additional information, such as the card holder's full name and address, mother's maiden name, date of birth, Social Security number, a PIN, and other personal information that allows additional criminal exploitation of the affected individual.

Although network intrusions can be devastating to a company of any size, the subsequent theft of data and customer information often has more dire consequences on a small or medium-sized company that most likely does not have the resources or expertise necessary to properly protect their networks and data. For example, in October 2007, the Secret Service identified a complex fraud scheme in which servers owned by a payroll company were compromised by a network intrusion. Subsequently, four debit card accounts belonging to a small Midwestern bank were compromised, distributed online, and used in a coordinated attack resulting in ATM withdrawals in excess of $5 million. The withdrawals involved 9,000 worldwide transactions in less than two days and the bank had to file for Chapter 11 bankruptcy protection. Our investigation revealed that the criminals compromised the payroll company's database, reset PINs, loaded balances onto the accounts, and removed account withdrawal limits or set the limits at extremely high levels.

Through this investigation, the Secret Service also identified another organized cyber-group in New York City trafficking stolen credit card data that was transmitted by multiple suspects operating in Russia and the Ukraine. Following the investigative leads generated in this case, the Secret Service was able to prevent additional losses by notifying victims of the intrusion and compromise, often before the victims became aware of the illicit activity. For example, the Secret Service discovered that the computer network of a U.S. bank had been compromised. Subsequent notification by the Secret Service enabled the bank to significantly reduce its exposure and avoid potential losses exceeding $15 million. Based on these investigative efforts, the Secret Service identified 15 compromised financial institutions, $3 million in losses, 5,000 compromised accounts, and prevented more than $20 million in potential losses to U.S. financial institutions and consumers.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals alike. Illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade in personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting memberships of approximately 8,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

Although increasingly difficult to accomplish, the Secret Service has managed to infiltrate many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the identification and high-profile indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers.

The investigation revealed that defendants from the United States, Estonia, China, and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

After they collected the data, the conspirators concealed the data in encrypted computer servers that they controlled in the United States and Eastern Europe. They then sold some of the credit and debit card numbers via online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraud proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

The total actual loss associated with this investigation is still being assessed. However, one of the corporate victims has already reported expenses of almost $200 million resulting from the intrusion.

In both of these cases, the ripple effects of the criminal acts extend well beyond the company compromised. In one example alone, millions of individual card holders were affected. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all of the potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Also, costs suffered by businesses, such as the need for enhanced security measures, reputational damage, and direct financial losses, are ultimately passed on to consumers.

Collaboration with Other Federal Agencies; State and Local Law Enforcement; Private Sector; and Academia

While cyber-criminals operate in a world without borders, the law enforcement community does not. The multi-national, multi-jurisdictional nature of these cyber-crime cases has increased in complexity and, accordingly, increased the time and resources needed for successful investigation and adjudication. For example, in the TJX investigation, the Secret Service not only worked with domestic law enforcement partners, but also with officials from Thailand, the United Arab Emirates, Turkey, Ukraine, Spain, Belarus, Estonia, and Germany. The complexity of this three-year investigation involved personnel from our San Diego, Miami, and Boston Field Offices working in close coordination with personnel from our Headquarters Divisions.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state, and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- National Protection and Program Directorate's (NPPD) – Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- Department of Homeland Security's Science and Technology Directorate (S&T);
- White House Homeland Security Staff;
- Department of Justice National Cyber Investigative Joint Task Force (NCIJTF);
- Each Federal Bureau of Investigation Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- National Security Council;
- The Drug Enforcement Administration's International Organized Crime and Intelligence Operations Center;
- EUROPOL; and
- INTERPOL

To continue to fulfill our obligation to protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled and continues to dismantle some of the largest known transnational cyber-criminal organizations by:

- providing the necessary computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program (ECSAP)**;
- collaborating with other law enforcement agencies, private industry, and academia through our 28 **Electronic Crimes Task Forces (ECTF)**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Criminal Intelligence Section (CIS)**;
- providing state and local law enforcement partners with the necessary computer-based training, tools, and equipment to enhance their investigative skills through the **National Computer Forensics Institute** (NCFI);

- maximizing partnerships with international law enforcement counterparts through our **international field offices**; and
- maximizing technical support, research and development, and public outreach through the Secret Service **CERT Liaison Program (CLP)** at Carnegie Mellon University.

Electronic Crimes Special Agent Program (ECSAP)

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP). This program is comprised of 1,148 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received extensive training in forensic identification, preservation and retrieval of electronically-stored evidence. ECSAP agents are computer investigative specialists and among the most highly-trained experts in law enforcement, qualified to conduct examinations on all types of electronic evidence. This core cadre of special agents is equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud, and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training and focus:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program is designed to provide Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations. The BICEP program has proven so effective that the Secret Service has incorporated it into its core curriculum for newly hired special agents.

Currently, the Secret Service has 823 special agents trained at the BICEP level.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers, or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Currently, the Secret Service has 161 special agents trained at the ECSAP-NI level.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence. The forensically obtained digital evidence is utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Currently, the Secret Service has 164 special agents trained at the ECSAP-CF level.

Electronic Crimes Task Forces (ECTF)

In 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state, and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress has since directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service has established 28 ECTFs, including the first international ECTF based in Rome, Italy. Membership in our ECTFs include: 299 academic partners; over 2,100 international, federal, state, and local law enforcement partners; and over 3,100 private sector partners. The Secret Service ECTF model is unique in that it is an international network with the capabilities to focus on regional issues. For example, the New York ECTF, based in the nation's largest banking center, focuses heavily on protecting our financial institutions and infrastructure, while the Houston ECTF works closely with partners such as ExxonMobil, Chevron, Shell, and Marathon Oil to protect the vital energy sector. By joining our ECTFs, all of our partners enjoy the resources, information, expertise, and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Criminal Intelligence Section (CIS)

Our Criminal Intelligence Section (CIS) collects, analyzes, and disseminates data in support of Secret Service investigations nationwide and overseas and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private partnerships to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has developed an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute (NCFI)

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, the Department of Homeland Security (DHS), and the State of Alabama. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations.

Investigators are trained to respond to network intrusion incidents and conduct basic electronic crimes investigations.

Since opening on May 19, 2008, the Secret Service has provided critical training to 564 state and local law enforcement officials representing over 300 agencies from 49 states and two U.S. territories.

Collaboration of International Partners

One of the main obstacles that agents investigating transnational crimes encounter are jurisdictional limitations. The Secret Service believes that, to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our foreign law enforcement counterparts. Currently, the Secret Service operates 22 offices abroad, each of which has regional responsibilities providing global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Computer Emergency Response Team (CERT)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program (CLP). The role of the CLP is threefold: (1) technical support; (2) research and development; and (3) public outreach and education.

The CLP is a collaborative effort with over 150 scientists and researchers engaged in the fields of computer and network security, malware analysis, forensic development, and training and education. Supplementing this effort is research into emerging technologies being employed by cyber-criminals, and development of technologies and techniques to combat them.

The objectives of the CLP are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen Secret Service partnerships and relationships with the technical and academic communities; to provide an opportunity for the Secret Service to work closely with CERT, SEI, and Carnegie Mellon University; and to provide public outreach and education.

Heartland Payment Systems Case

As an example, the partnerships developed through our ECTFs, the support provided by our Criminal Intelligence Section, the liaison established by our overseas offices, and the training provided by ECSAP were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems (HPS). An August 2009 indictment alleges that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer" to capture payment transaction data.

The Secret Service investigation revealed data from more than 130 million credit card accounts at risk of being compromised and ex-filtrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including search warrants, the use of Mutual Legal Assistance Treaties with our foreign law enforcement partners, and subpoenas to identify three main suspects. As a result of this investigation, the three suspects in the case were indicted and charged with various computer-related crimes.

This case represents the largest and most complex data breach investigation ever prosecuted in the United States.

Conclusion

Today, hundreds of companies specialize in data mining, data warehousing, and information brokerage. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals. However, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted. The Secret Service and DHS continue to collaborate closely with the private sector to improve coordination and communication on cyber issues.

As I have highlighted here, the Secret Service has implemented a number of initiatives on cyber and computer-related crimes. Responding to the growth in these types of crimes and the level of sophistication these criminals employ demands an increasing amount of resources and greater collaboration. Accordingly, we dedicate significant resources to increasing awareness, educating the public, providing training for law enforcement partners, and improving investigative techniques. The Secret Service is committed to our mission of safeguarding the nation's critical infrastructure and financial payment systems. We will continue to aggressively investigate cyber and computer-related crime to protect consumers.

In conclusion, I would like to reiterate that cyber-crime remains an evolving threat. It is not a threat of the future; it is very much here. Law enforcement agencies must be able to adapt to emerging technologies and criminal methods. The Secret Service is fully involved in the federal government's new approach to cybersecurity. We are dedicated to the government's collective effort to adopt innovation in our approach to cyber-crime and cybersecurity and to stay ahead of this ever-changing threat. The Secret Service is pleased that the Committee recognizes the magnitude of these issues and the constantly changing nature of these crimes; to effectively fight this crime, our criminal statutes must be amended to safeguard sensitive personally identifiable information and to afford law enforcement the appropriate resources to investigate data breaches.

Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Statement for the Record

Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
September 14, 2009

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for inviting me to appear before you today to discuss the work of the Department of Homeland Security (DHS) to improve the Nation's cybersecurity. The Committee's topic, "Cyber Attacks: Protecting Industry Against Growing Threats," is quite possibly the most critical and complicated matter on the Nation's cybersecurity agenda. The security of private sector information, systems, and networks is essential for the activities of today's businesses and consumers. And, since much of our nation's critical infrastructure is in industry hands, ensuring the security of private-sector cyber resources is a vital part of the Nation's overall cybersecurity.

The President has developed a coordinated approach to cybersecurity which elevates cybersecurity in the White House. This approach includes the appointment of a Chief Technology Officer, located in the Office of Science and Technology Policy, a Chief Information Officer in the Office of Management and Budget, and the pending appointment of a cybersecurity policy official in the White House. This team provides an effective means for coordination and collaboration – across the Federal government and with the private sector - underscoring the high priority the administration places on securing cyber space. At DHS we work closely on all cybersecurity matters with this leadership team and the rest of the federal agencies to ensure a coherent, coordinated approach with the private sector.

DHS has both broad and specific responsibilities for cybersecurity. Secretary Napolitano has designated me as the focal point and coordinator for DHS's cybersecurity responsibilities, both in my role as the Deputy Under Secretary of the National Protection and Programs Directorate (NPPD) and as the Director of the National Cyber Security Center. Specifically, DHS has responsibility for enabling the Federal civilian agencies to secure their information, systems, and networks. Additionally, we lead the Federal Executive Branch's work with America's private sector to secure the communications and information infrastructure critical to our economy and way of life. This infrastructure, sometimes referred to as the dot com domain, is largely owned and operated by the private sector. As a result, DHS and the broader Federal Government must rely on our private sector partners as we work to ensure that resiliency, security, privacy, and other critical protections are built into our evolving infrastructures.

While today's hearing focuses on our work with the private sector, we are also very concerned with protecting the dot gov domain. I look forward to talking with Committee about those activities in the near future. And, as the testimony of Assistant Director Merritt of the United States Secret Service illustrates, DHS has other missions and capabilities in the cybersecurity domain. In all this work, DHS requires and receives strong support from the White House, Congress, and the Federal agencies that own and operate their own systems or are the subject matter experts and regulatory contacts for specific parts of the private sector.

My current activities reflect three top priorities. The first priority is building capacity – primarily human, but also technical capacity – within DHS. With excellent support from the Administration and Congress, we have grown aggressively over the past several years to build a world-class, sustainable cybersecurity workforce that can successfully address this complex and growing challenge. Much of this workforce is focused on our mission to secure the dot gov (Federal civilian agency) domain. This includes leading a number of activities under the Comprehensive National Cybersecurity Initiative and the Administration's Cyberspace Policy Review. As the Committee knows, Federal information technology (IT) systems are under constant attack—via the Internet and other means—from individuals and groups that seek to disrupt, deny access to, degrade, or destroy those systems and the data contained on them. A comprehensive Federal network defense entails: situational awareness of the state of networks; an early warning capability; near real-time and automatic identification of malicious activity; and the ability to deflect or disable malicious activity before harm is done. DHS, through the National Cyber Security Division, is developing a system-of-systems approach that encompasses the people, activities, processes, and technologies needed to fulfill its cybersecurity mission. DHS is implementing the Trusted Internet Connection initiative, a multi-faceted program for improving the Executive Branch's cybersecurity posture by reducing the number of external internet connections. Further, we are leading the deployment of the EINSTEIN program, which is creating intrusion detection and prevention capabilities on Federal networks. In this, as in all our work, enhancing the privacy and civil liberties of the American public is at the core of our strategy and approach.

My second priority is building partnerships with key stakeholders inside and outside government, including strengthening our working relationships with the private sector on all levels. I will briefly highlight specific examples of our work with the private sector, they are as follows:

Incident Response

The President's Cybersecurity Policy Review calls for "a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident." DHS has the lead for this initiative; we are managing a working group comprised of representatives from the private and governmental (Federal, State, and local) sectors to develop a National Cyber Incident Response Plan (NCIRP). This will produce a clear delineation of roles and responsibilities in case of a major cyber incident, and it will update the Cyber Incident Response Annex to the National Response Framework created under Homeland Security Presidential Directive 5. Most importantly, we have launched this process with the private sector integrated from the very start to establish an actionable response framework that will allow us to respond to a cyber incident as one Nation, not just as one government. In concert with the NCIRP, we are designing and developing a DHS-managed alert and warning system for cyber-related incidents as well as updating concepts of operations, standard operating procedures, and playbooks.

A key part of successful incident response is the ability to coordinate operations across multiple organizations. In this regard, DHS is building an integrated cybersecurity and communications watch floor that will collocate the capabilities of various DHS cybersecurity and communications-related response organizations. This joint watch floor, which will be operational before the end of 2009, will also provide additional capacity for State and local government and private sector participants to be physically and virtually present at the front lines of the national response, strengthening capability and building trust though operational activity. This consolidation of capability has been recommended by the President's National Security Telecommunications Advisory Committee (NSTAC) and by other expert groups.

We expect to test the NCIRP early next year and exercise it, with substantial participation from the private sector, during the Cyber Storm III exercise in September 2010.

Advisory Groups

Enormous cybersecurity expertise resides in the private sector, in the information and communications technology industry, and within the critical infrastructure sectors. DHS sponsors a variety of advisory groups pertinent to cybersecurity issues. These include two Presidential advisory committees -- the NSTAC and the National Infrastructure Advisory Council -- and a variety of DHS-specific committees and working groups under the framework of the Critical Infrastructure Partnership Advisory Council.

The Cross-Sector Cyber Security Working Group, for example, is a DHS-specific committee working to facilitate the bi-directional sharing of operational cybersecurity information within and across critical infrastructure sectors and government agencies, including indications and warnings in advance of incidents. In addition, the Information Technology Sector Coordination Council and DHS co-published the IT Sector Baseline Risk Assessment in August 2009, providing the basis for identifying IT risks to national and economic security, public health and safety, government services, and the operation of other critical infrastructure. It is an all-hazards risk assessment that provides an evaluation of the IT sector's threats, vulnerabilities, and consequences and informs the development of strategies to mitigate sector-wide risks. This baseline assessment is an example of how government and industry can collaboratively create a basis for making more informed decisions about security.

There are finite resources in both government and industry to address ever-changing and emerging requirements; we must collectively make the most efficient use of our energies. In order to ensure that DHS is working most efficiently, we are reviewing the roles and responsibilities of the various advisory bodies in order to determine how to most effectively utilize the time and commitment of the private sector in this complex arena and ensure that the Government is best able to implement their recommendations.

Information Sharing

As suggested above, the sharing of cybersecurity information, indications, and warnings between government and the private sector can prevent or mitigate the consequences of attacks. For example, when DHS' 24/7 watch and warning center, the United States Computer Emergency Readiness Team (US-CERT), becomes aware of potential or ongoing efforts to compromise government and private sector systems, it shares this information with federal and industry partners. This information sharing helps prevent or minimize disruptions to critical information infrastructures and protect the economy, government services, and the national security of the United States. US-CERT has released more than 40 alerts and products during the first eight months of 2009. The products are used by many public and private sector entities, domestically and internationally, to increase the security of their networks and data.

US-CERT is taking steps to improve its capabilities in this area. For example, US-CERT recently developed the Joint Agency Cyber Knowledge Exchange (JACKE), a secure conference call/meeting among cyber and IT analysts and engineers, to improve situational awareness and recommend actions for Federal agency security operation centers. Fifteen agencies are participating, and our next step is to expand participation in JACKE to include all 26 major departments and agencies. We believe this effort will produce or influence products that will be helpful to the private sector as well.

Further, earlier this year, DHS hosted an Industry Day to highlight the need for private industry to become more involved in developing comprehensive, game-changing, innovative solutions that improve and expand upon current capabilities. As a follow-up, DHS released a request for information to the private sector to identify prospective private sector technical, end-to-end solutions for protecting the Federal cyber domain.

Cybersecurity Awareness

In October, we will mark the sixth annual Cybersecurity Awareness Month. This year's focus is on promoting shared responsibility for cybersecurity among all stakeholders, including the creation of a culture of cybersecurity in organizations. As in past years, DHS is working with stakeholder organizations such as the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center to expand our reach into to the private sector both on a nationwide and state-by-state basis.

Cyber Crime

I want to touch briefly on cyber crime, given the composition of the rest of today's panel. For most private sector organizations, and especially for small businesses, attacks by cyber criminals trying to steal businesses' financial resources are the greatest and most proximate cybersecurity concern. Cyber criminals have moved far beyond the mere disruption and hacker reputation building activities of a bygone era—cyber criminals now look for money and value. There are many simple steps that businesses can and should take to protect themselves. Securing the entrances of one's factory or store is second nature to any business owner and so cyber security protections must become. A recent public report from Verizon's business risk team estimated that 87 percent of data breaches could be avoided by simple to intermediate preventative measures. And yet many small businesses do not keep their virus protections or firewalls up to date. Simple hygiene of this type can go a long way to preventing cyber crimes. US-CERT provides valuable tips and guidance at www.us-cert.gov, as well as links to other resources.

Finally, my third priority looks to the long term, we are anticipating and driving change in the public-private cyber ecosystem. For example, we intend to:

- Work with our partners across the government and private sector to ensure that: incentives and requirements for security align with national and homeland security needs; metrics enable distributed actors to make judgments about security based on data; and future architectures meet national needs for security and resiliency, including in the areas of software assurance, supply chain protection, and risk assessment;
- Build interoperability in communications and information for confidentiality, integrity, and availability;
- Work with partners in government and critical infrastructures to create and implement a vision and system that will enable the authentication of people, processes, and devices, protecting privacy by design and mitigating major categories of threats and threat actors; and
- Build cybersecurity both as a profession and as a core element of other professions, equipping the next generation of leaders and operators to succeed.

Conclusion

The Nation's critical networks and systems are vulnerable to a persistent, evolving and sophisticated cyber threats. DHS, in conjunction with its public and private sector partners, is at the vanguard of the efforts to secure those networks and systems. With the support and leadership of the White House, Secretary Napolitano has focused the Department so that cybersecurity will receive the high-level attention it merits.

We cannot solely pay attention to today's challenges. The dynamic cybersecurity environment demands constant innovation, and we are collaborating with others to anticipate future cybersecurity challenges so that we can outpace our adversaries. DHS is building a holistic, comprehensive, long-term cybersecurity vision and strategy that relies on a collaborative approach. A key component of that effort is building a world-class cyber workforce to meet the demands of both today and the future. We must also build awareness and understanding of cybersecurity issues among the public. While DHS has already built a robust public-private cyber partnership, we expect that partnership to continue to mature. There is much more work to be done and we must all work together if we are to accomplish the mission. I look forward to working with this Committee in that effort.

Thank you, and I would be pleased to answer any questions.

Post-Hearing Questions for the Record
Submitted to Philip R. Reitinger
From Senator Susan M. Collins

"Cyber Attacks: Protecting Industry Against Growing Threats"
September 14, 2009

1. Many small and mid-size businesses are using computer software to manage their business that is bought right off a store shelf. They are using the same operating systems and word processing applications that individuals would use at home. Thus, unlike large buyers like the Federal government or Fortune 500 companies, these businesses have little leverage to demand better security in those products.

   Mr. Reitinger, you come to the Federal government from one of the largest software manufacturers in the world and so can offer a unique perspective for us. How can we help give small and mid-size businesses the same sort of leverage that large companies have to influence the development of products with better security?

Response: Because we are talking about commercial-off-the-shelf software, the question is less about giving individual small and medium-sized businesses leverage and more about enabling the broader market to provide that incentive to develop easy-to-use technology that can help these businesses secure their networks, systems and data. We can do this in at least three ways. First, we can ensure that government acquisition of software and Information Technology services take security appropriately into account. Second, we can work with industry and across the Government to develop best practices, curricula, and other materials that help software producers develop more secure products and educational institutions to produce better software developers. Third, we can help to build the right metrics so that companies, large or small, can make good decisions about what software to deploy on their networks and systems. Through the Department of Homeland Security's Software Assurance Initiative and partnerships across the Government and with industry, we are working toward these ends, while at the same time, helping to give all consumers access to those security-enhanced products and services.

CADNA
The Coalition Against Domain Name Abuse

Testimony of Josh Bourne
President and Co-Founder
Coalition Against Domain Name Abuse
Before the Committee on Homeland Security and Governmental Affairs

Hearing on Cyber Attacks: Protecting Industry Against Growing Threats
September 14, 2009

Mr. Chairman and distinguished members of the committee, thank you for convening this timely hearing on issues concerning cybersecurity. Today, there are over 1.5 billion users of the Internet, but it is likely that less than one percent of the users are even aware that Internet policy is set by the Internet Corporation for Assigned Names and Numbers (ICANN), let alone how the drastic changes ICANN is about to implement will dramatically impact the space. Given the commercial significance of the Internet and the potential national security threats possible through the Internet, it is critical that the United States Congress involve itself in matters of domain name space policy and regulation.

My name is Josh Bourne and I am the president and founder of the Coalition Against Domain Name Abuse (CADNA). CADNA, a 501(c)(6) non-profit association, was founded over two years ago with the help of Fairwinds Partners and leading brand owners to combat a variety of abuses on the Internet. CADNA represents businesses vital to the American and global economies, including American International Group, Inc., Bacardi & Company Limited, Carlson/Carlson Hotels Worldwide/Carlson Restaurants Worldwide, Compagnie Financière Richemont SA, Dell Inc., DIRECTV, Inc., Eli Lilly and Company, Goldman, Sachs & Co., Harrah's Entertainment, Inc., Hewlett-Packard Company, Hilton Hotels Corporation, HSBC Holdings Plc, InterContinental Hotels Group, Marriott International, Inc., New York Life Insurance Company, Nike, Inc., Verizon Communications, Inc., Wells Fargo & Company, and Wyndham Worldwide Corporation.

CADNA was founded in response to the growing international problem of cybersquatting, which is the bad faith registration of a domain name that includes or is confusingly similar to an existing trademark. Because attracting Web traffic is vital to success in the online space, the loss of users due to negative impressions may bear significant consequences for a company. In addition to the mounting legal costs that companies now face in defense of their own domains, this infringement costs organizations billions of dollars in lost or misdirected revenue. Furthermore, cybersquatting harms Internet users by creating confusion; infringing domains that potential customers happen upon could be set up by cybersquatters to deposit spyware or malware or host phishing schemes. According to a survey conducted by Gartner, Inc., the average phishing victim in the United States lost $866 in 2007, with total losses from phishing attacks soaring to $3.2 billion. Infringing sites could also be set up to intercept emails meant for the proper brand owner, which could contain sensitive information.

CADNA works to decrease instances of cybersquatting in all its forms by facilitating dialogue, effecting change, and spurring action on the part of policymakers in the national and international arenas. CADNA also aims to build awareness about illegal and unethical infringement of brands and trademarks online.

CADNA seeks to make the Internet a safer and less confusing place for consumers and businesses alike. Taking action against the practices of cybersquatting, CADNA provides a framework for brand owners to protect themselves—as well as their investors, customers and partners—from illegal trademark infringement.

Thank you very much for the opportunity to present the views of our organization on this very important topic.

With the Joint Project Agreement (JPA) set to expire on September 30 and reports of a possible new agreement being negotiated to take its place, we feel that it is critical for the Internet community and the US government to pause, take a step back, and reassess the success of ICANN, the not-for profit organization that has day-to-day responsibility for establishing policies and managing the operations of the Internet's domain name system (DNS). ICANN's policies have produced an online environment favorable for cybersquatting, fraud and other nefarious activities.

ICANN is failing to address numerous issues corrupting the Internet: ICANN often ignores issues regarding the safety and stability of the Internet, such as the proliferation of cybersquatting, which can enable phishing, malware deposit schemes, and the sale of unwanted counterfeits. ICANN has also largely ignored the problem of inaccurate WHOIS information, which encumbers the identification and prosecution of bad actors. Rather than helping to make the Web more secure, ICANN is increasing the online risks that businesses and consumers face by irresponsibly releasing new generic top-level domains (gTLDs).

When US policy was developed in the late 1990s, the United States Government thought that by September of 2009 ICANN would exist as a transparent and reliable force for sensible and practical policies for the Internet. Unfortunately, this has proven not to be the case, and so governments must rethink its stance towards ICANN in a thoughtful and considered manner.

CADNA
The Coalition Against Domain Name Abuse

Members of the global business community believe that while ICANN has achieved many things, broad participation and involvement of its diverse stakeholders is not one of them. To date, those involved in ICANN policy have not represented the needs of users and user groups that utilize and depend on the Internet in widely varying respects. There is a lack of diversity, cross-constituency interaction, and overall balanced debate and discussion present in ICANN's day-to-day policy development and in international meetings, leaving much to be desired. For example, ICANN recently adjusted the voting structure of its policy-making body, the Generic Names Supporting Organization (GNSO), so that those with financial interests have a majority of the vote rather than allowing all Internet-using constituencies equal participation. While Internet users, businesses, and governments have slowly begun to take a greater interest in the domain name space, we fear that ICANN's current framework does not offer adequate opportunities or incentives to encourage broader involvement. It also does not allow for the development and implementation of good policy.

Unfortunately, ICANN has often fallen short of its duty to maintain the stability, reliability, and security of the Internet and tends to favor certain special interests rather than looking out for the diverse interests of the global Internet community. One prime example of this is the decision to open up the Internet to the creation of a limitless number of extensions, which benefits the very entities that control the GNSO- registrars and registries. Registrars and registries have long been working through ICANN to create policy to regulate the very product that they sell; it is no wonder now that they are pushing for a policy that will give them an unlimited supply of their product, regardless of that product's impact on the market.

CADNA does not claim that there should never again be another gTLD launch; it may very well be true that a new gTLD can provide innovation to the domain name space. However, opening up the floodgates to a potentially unlimited number of gTLDs, with many of ICANN's own staff uncertain about the scalability of operations and with the current domain name space plagued with problems, is dangerous and irresponsible.

ICANN's plans to dramatically increase the number of website names available for registration will make the web exponentially more complex. Given the state of the current domain name governance system, priority should be given to correcting existing issues rather than expanding the space. For example, it is still too easy for cybersquatters to register domain names in bad faith that are lawfully associated with legitimate entities. Even without these proposed gTLDs, cybersquatting grew by 18% in the last quarter of 2008.

Cybersquatters are also extremely difficult to apprehend as a result of ineffectual ICANN policies. ICANN is aware of the fact that its requirements regarding WHOIS information are weak, leading to faulty or inaccurate information about the identities of cybersquatting domain name owners, but it has yet to adjust its policies. New gTLDs would only exasperate this problem. Rather than allowing this issue to go unchecked, ICANN should resolve it before increasing the size of the domain name space and the opportunities to practice fraud.

Conservative estimates put the average cost per sunrise registration around $300. If a typical company registered 20 domains in each sunrise period, the cost to participate in all 200 new gTLDs that could be added in 2010 would be $1.2MM. The costs of participating in new gTLD launches can be much greater than outlined above due to offers of special registrar queues to raise probability of successfully registering a domain, extra validation services, and gimmicky programs presented by new registries. Furthermore, as with gTLDs such as dot-MOBI, dot-EU and dot-ASIA, companies may feel compelled to defensively register hundreds of domains rather than a mere 20.

If brand owners chose to participate in just 10% of the new gTLDs to be launched in 2010, the average expenditure per brand just for 20 trademark sunrise registrations in each could be $120,000. This represents a steep 37.5 per cent cost increase since the average company spends less than $200,000/year maintaining their domain portfolio.

Brand owners who are already under water due to infringements in the 1000+ worldwide domain extensions will be forced to contend with the added complexity of policing the use of their brands in domain names. The costs of monitoring and enforcing the new gTLDs are likely to be significant. This is not to mention the brand dilution, proliferation of cybercrime and damage to the integrity of the Internet that are sure to occur. These new gTLDs will afford the most benefit to domain industry insiders, criminals and others that look to profit in an expanded Internet real estate market.

Below is a simple summary of the cost to businesses and consumers that a proliferation of gTLDs will create:

- An average company will spend $40,000 per year for online and domain monitoring
- Cybersquatting will grow at a rate of 100% year after year
- On average, a global corporation will face 5,000 infringements every year
- 50% of all cybersquatting sites receive meaningful traffic
- Cybersquatting sites that garner meaningful traffic receive an average of 600 visitors/year
- 25% of visitors to Pay-Per-Click (PPC) sites click on the posted links

CADNA
The Coalition Against Domain Name Abuse

- Of those who click on PPC sites, 75% click on the link provided and paid for by the brand owner represented in the domain name
- Average cost per click is $.50 (conservative est. since clicks can be 10+ times this amount)
- An average company files 10 Uniform Dispute Resolution Policy (UDRP) complaints per year (one domain per UDRP)
- The average total cost of each UDRP is $5,000
- An average company sends 150 cease and desist letters annually (assuming a 100% success rate)
- Cost per cease and desist letter is $50 (even if generated in-house)

*These estimates do not include an estimate regarding the loss of sales or damage to brand value that occur as a result of cybersquatting activities.

It is important to remember that the average Internet user—every individual that uses the Internet for personal or business use—is also a victim of the current space. As a result of ICANN's policies, there is a lack of transparency, accountability, and security online, so as Internet users continue to be vulnerable to phishing, malware deposits, diversion, and confusion there remains little opportunity for recourse and retribution. This would only expand exponentially along with any gTLDs that would be added.

Thank you for your time and consideration on this very important matter.

Sincerely yours,

Josh Bourne
President, Coalition Against Domain Name Abuse

○