S. Hrg. 112–221

PROTECTING CYBERSPACE: ASSESSING THE WHITE HOUSE PROPOSAL

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 23, 2011

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

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

U.S. GOVERNMENT PRINTING OFFICE

67–638 PDF WASHINGTON : 2012

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE MCCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*
JEFFREY E. GREENE, *Senior Counsel*
MATTHEW R. GROTE, *Professional Staff Member*
NICHOLAS A. ROSSI, *Minority Staff Director*
BRENDAN P. SHIELDS, *Minority Director of Homeland Security Policy*
DENISE E. ZHENG, *Minority Professional Staff Member*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

WITNESSES

MONDAY, MAY 23, 2011

ALPHABETICAL LIST OF WITNESSES

APPENDIX

PROTECTING CYBERSPACE: ASSESSING THE WHITE HOUSE PROPOSAL

MONDAY, MAY 23, 2011

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

The Committee met, pursuant to notice, at 10:33 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, and Collins.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Thanks to everyone for being here. Thanks particularly to the representatives of the Administration who are before us as witnesses.

If there is anyone who does not believe that we urgently need to pass strong cybersecurity legislation, which is the topic of our hearing today, I would tell them to look at some of the high-profile computer attacks that have happened in the past several months, that is, the ones that we know about.

Let us just take the Sony Corporation as an example. In two separate attacks, hackers stole the personal and billing information, including reportedly some of the credit card numbers, of 100 million people. And when the Sony site finally reopened last Thursday, the company found that they had not actually been able to close all the vulnerabilities that had been opened up in the wake of the first two attacks and that hackers could still use the information to hijack users' accounts.

If that does not convince skeptics we have a real cybersecurity problem in America, then consider the breaches that have occurred in the cyber systems of organizations that specialize in cybersecurity. Take our own Oak Ridge National Laboratory, which has a very important role in fulfilling the Department of Energy's responsibility to secure our electric grid from cyber attack, whether by enemy nations or cyber terrorists. Oak Ridge National Laboratory was itself successfully cyber attacked just last month.

Or one that has been widely described in the media, RSA, a company whose SecurID program is used by about 40 million entities, users, really, at 30,000 companies, including parts of the Federal Government. And those parts include the Social Security Administration, the Department of Defense (DOD), and the U.S. Senate. RSA had valuable security information stolen from its computers

that could compromise these systems and actually be used in future attacks.

So, bottom line—and these are just a few examples, and again, these are examples that are on the public record—if we do not do something soon, the Internet is going to become a digital Dodge City. Cyberspace is just too important to modern life for us to sit back and allow that to happen. This is a place that really cries out for law. It is time to say, if I may continue the Dodge City metaphor, that there is a new sheriff in town and we are going to have some law and order around here, and we could do that, of course, without compromising, in effect, alongside elevating liberty and privacy.

The recent release of the White House's proposed cybersecurity legislation is a very important step in that direction. I think it represents a turning point in our efforts to pass the strong measures we need to protect consumers, businesses, critical infrastructure, and our national security from cyber attack by terrorists, spies, or crooks.

I am pleased not just by the appearance of the Administration's cybersecurity legislation, but by its substance. The President's proposal is similar in many ways to legislation this Committee reported out earlier in this session of Congress, and where there are differences, I think we can work together to find agreement. So I am, in this regard, very grateful to the witnesses for appearing before us today. This is the first public testimony that the Administration has given on its cybersecurity proposal since it was released.

One important area of agreement is the recognition that the Department of Homeland Security must be given the job of protecting the "dot-gov" and "dot-com" domains. In other words, the Department of Homeland Security (DHS) will be the new sheriff in cybertown that we need. A crucial part of this job will be for DHS to identify critical cyber infrastructure, the systems or assets that control things like power plants, electric grids, and pipelines that, if commandeered by our enemies, could lead to havoc and, of course, death and destruction. DHS needs that authority and also the ability to evaluate the risks to those systems.

Once the systems and risks have been identified, their owners and operators, under the proposal that we have made, will be required to develop plans to safeguard their systems. Those plans will be reviewed to ensure they will actually improve security, reviewed in our proposal by the Department of Homeland Security, in the White House proposal by government-accredited third-party evaluators.

Just last week, if I may say, in our role as oversight Committee of the Department of Homeland Security, that we saw an example of why this kind of planning is so necessary and why the Department of Homeland Security has raised itself to a quality of performance that it deserves to have the job. A private researcher apparently discovered a major security flaw in a widely-used industrial control system and planned to present this research at a conference. When personnel at the Department of Homeland Security discovered this and explained to the researcher how dangerous it would be to have this information out in public before the security

VerDate Nov 24 2008 11:37 Feb 08, 2012 Jkt 067638 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 P:\DOCS\67638.TXT SAFFAIRS PsN: PAT

flaws had been patched, he voluntarily canceled his talk. This is very important because another cybersecurity expert said of this particular vulnerability, "This is different from simply stealing money out of someone's bank account. Things could explode."

Besides securing critical infrastructure, our bill and the White House bill would direct the Department of Homeland Security to work cooperatively and on a voluntary basis with the private sector and State and local governments to share cybersecurity risk and best practice information.

The White House proposal also clears the way for industry to share cybersecurity information without having to worry about running afoul of various privacy statutes that impede information sharing now. The business and government communities would be free to use this advice as best suits their needs. There would be no one-size-fits-all mandates or dictates.

Both the White House bill and our Committee bill also contain robust privacy oversight to ensure that our broader cybersecurity efforts do not impact individual privacy or civil liberties.

And finally, both our proposals would also reform and update the Federal Information Security Management Act (FISMA) to require continuous monitoring and protection of our Federal computer networks and to do away with the current paper-based reporting system.

Now, one key difference between our bill and the White House proposal is that our legislation creates a White House Office of Cyberspace Policy with a Senate-confirmed leader. We believe that the stakes are so high when it comes to cybersecurity for our country that whoever holds that position should be confirmed by the Senate and, therefore, accountable to Congress.

Our Committee's bill would also clarify the President's authority to act in the event of a true cyber emergency while at the same time ensuring that the President cannot take any action that would limit free speech or shut down the Internet. In its original version, this section was, in our opinion, misconstrued, and we have tried in the language that was reported out of Committee to reassure everybody about the limitations, the very limited circumstances under which the President could act and the limited range of his actions.

The Administration, on the other hand, and I will be interested in discussing this, believes that additional statutory authority in this regard is unnecessary because the President has the authority that we give him in this proposal already in existing law.

Bottom line, the Internet is a thrilling new frontier of our age, with a plugged-in population of almost two billion now, and that number is growing every day. The Internet has created a revolution in commerce, communications, entertainment, finance, and government, really, just about every aspect of our lives. But what we are saying is that it must not be a lawless frontier. I believe that with the proposals we have in front of us, we can bring about the needed change this year to make the Internet safer and more secure.

The Majority Leader, Senator Harry Reid, has taken a very active interest in this legislation. It remains a priority of his for this session. I have said to him that I believe it is the most important

piece of legislation coming out of our Homeland Security Committee in this session. He is working, I am pleased to say, with the Republican leader, Senator Mitch McConnell, as Senator Collins and I, of course, have worked together here. There are five or six different committees of the Senate that claim some part of the jurisdiction over this subject matter, and I believe it is the intention of the bipartisan leadership of the Senate to establish a process by which all those Committees can, as quickly as possible, negotiate any remaining differences in the bills that have come out of committee so that we can bring it to the Senate floor as quickly as possible.

We have had a very successful round of negotiations with the Commerce Committee, which is the other committee claiming major jurisdiction here, and we have resolved just about all of the differences, not every one, but just about every one that we had between us.

Now, before I yield to Senator Collins, I want to just take a moment to thank Phil Reitinger, who, as Deputy Under Secretary of the National Protection and Programs Directorate has done a great job in a relatively short period of time, really elevating the quality of the cybersecurity operations at DHS and has been a real leader in crafting this White House proposal, including working very productively and cooperatively with our Committee. So we thank you for that, Mr. Reitinger.

With the bill finalized, as I suppose most people in the room know, Mr. Reitinger has decided to move on to the next great chapter of his life. I am not going to put him under oath to have him declare exactly what that will be yet, but whatever it is, we wish you well and thank you for your public service, which has made a real difference to our country.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Let me begin by saying that I am very pleased that the Administration is now fully engaged on the imperative issue of drafting and passing cybersecurity legislation. Experts tell me that the cyber arena is where the biggest gap exists between the threat level and vulnerabilities and our level of preparedness.

Virtually every week, we learn of another massive cyber breach. The company that authenticates users seeking to access Senate networks was hacked. As the Chairman has indicated, Sony's online gaming network was breached. This morning, we read in our newspapers that the repressive government of Syria attacked the social media sites of dissidents and protesters.

The truth is that the number and sophistication of cyber attacks continue to grow each and every day. The Federal Bureau of Investigations (FBI) reports that small and medium-sized businesses in our country lost more than $11 million over the past year in online scams in which stolen banking credentials were used for fraudulent buyer transfers to Chinese companies. Worldwide, the annual cost of cyber crime has climbed to more than $1 trillion. And according to the alarming testimony last year from the office of the Senate Sergeant at Arms, on average, each month, 1.8 billion cyber attacks

target the computer systems of Congress and the Executive Branch.

Unfortunately, the government's overall approach to cybersecurity has been disjointed and uncoordinated to date. The threat is simply too great to allow this to continue. The need for Congress to pass comprehensive cybersecurity legislation is more urgent than ever.

So I am pleased that the White House has now joined the efforts that this Committee has undertaken over the past few years to develop a bill to help safeguard the American people from a cyber September 11, 2001. I am also encouraged that the Administration's approach is similar in many respects to our framework. Both bills call for a strong public-private partnership to improve cybersecurity. Our bill would bolster sharing within the private sector and across government of actionable threat intelligence that would help protect the private sector from advanced cyber threats. It would also direct the Department of Homeland Security to collaborate with the private sector to develop and promote cybersecurity best practices.

Like our bill, the White House proposal recognizes that the Department of Homeland Security should be the appropriate agency to lead the Federal effort to secure Federal civilian agencies, the dot-gov domain, as well as the critical infrastructure in the private sector and public sector against cyber threats.

I believe that cybersecurity at DHS must be led by a strong and empowered director who can close the coordination gaps that now exist. This leader should report directly to the Secretary of Homeland Security and also serve as the principal adviser to the President on cybersecurity. To me, the best construct, which is not included in the White House proposal, is modeled on the National Counterterrorism Center and would apply a multi-agency approach to this issue that would be within DHS, and I look forward to exploring that issue with our witnesses this morning.

On a positive note, the Administration's approach to securing our Nation's most critical infrastructure is very similar to the risk-based approach in our bill. Our bill differs, however, in providing liability protection as an incentive for companies to maintain continuous compliance with risk-based performance requirements.

We should also detail the extent of the President's authority to deal with cyber emergencies. As the Chairman has pointed out, our bill has explicit provisions preventing the President from shutting down the Internet. It also places limits on the length of any emergency actions, requires reporting to Congress, ensures remedial actions are the least disruptive steps feasible, and includes privacy protections. By contrast, and I must say this baffles me, the Administration appears to be relying on outmoded yet potentially sweeping authorities granted in the Communications Act of 1934. I want to emphasize that date to point out just how outmoded those authorities are.

Our bill explicitly calls for the development of a supply chain strategy to leverage the Federal Government's buying power to drive improvements in cybersecurity. This would have beneficial ripple effects in the larger commercial market. As a very large customer, the Federal Government can contract with companies to in-

novate and improve the security of their information technology (IT) services and products. These innovations could lead to new security baseline for services and products offered to the private sector and the general public without mandating specific market outcomes.

In addition, our bill would give DHS the authority to hire and retain highly qualified cybersecurity professionals.

I look forward to discussing these important issues with our witnesses today, but most of all, to working together to finally secure the passage of comprehensive cybersecurity legislation.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. Thank you very much.

Senator Carper has been a cosponsor with Senator Collins and me of the legislation originally introduced, particularly with interest over the longer haul in the FISMA part of the bill, but overall, and I would welcome an opening statement from you at this time.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. I am delighted to give one. As the clock was ticking down into this weekend and we were approaching the end of the world——

Chairman LIEBERMAN. Yes. [Laughter.]

Senator CARPER [continuing]. I was thinking, we worked so hard to try to develop consensus on this Committee——

Chairman LIEBERMAN. Right.

Senator CARPER [continuing]. With the Commerce Committee, and with the Administration. It would really be a shame if it all ended before we got this done.

Chairman LIEBERMAN. It could be that is why it did not end.

Senator CARPER. The good news is we are all still here. The bad news is, so are the hackers that are trying to get into our bank accounts and steal our secrets, whether military secrets or all kinds of trade secrets, innovation secrets. I guess if you had to choose between one outcome or the other, this is probably the better outcome, and I am pleased that we have some consensus that is building. I really want to thank both of you for helping to spearhead that.

I am delighted that we are moving swiftly to hold this hearing on the Administration's proposal to improve our Nation's ability to defend against cyber attacks, and I ran into a couple of these fellows earlier this morning coming into the Dirksen Building. One of them actually had his father in tow, and we especially welcome him and thank him for sharing his son with us.

It has now been nearly 10 years since September 11, 2001, and over that period of time, our country has done a tremendous amount of work to defend against the kinds of attacks that we saw that day. We started with our airports, launching pad of the destruction the September 11, 2001 terrorists inflicted upon us, and under your leadership, Mr. Chairman, and the leadership of Senator Collins, we then dramatically reorganized our government to better prevent attacks and prepare for the consequences of both natural and manmade disasters. We have also worked to better se-

cure our ports, our mass transit systems, our chemical facilities, and other key pieces of our infrastructure.

Today, the architect of September 11, 2001, is dead. And while we still face many threats, I think we can say that our country is, in a number of ways, safer, I think maybe much safer, than it was on September 10, 2001. That does not mean we sit back and take it easy. We are not going to do that. But we do face a new threat today that I do not think was even on our radar screen 10 years ago. More and more Americans live their lives and conduct their businesses online, and this has created an attractive target for hackers and criminals looking to steal information or money or just to cause mischief.

At the same time, we have an increased reliance on sophisticated technology to keep the lights on, keep our water clean, run our factories, and even to fight wars and defend our country. Terrorists with the ability to compromise and damage or destroy the technology we depend on every day could cause serious damage, potentially even on the scale of a cyber September 11, 2001.

In past congresses, I have introduced legislation that would begin the process of addressing our cyber vulnerabilities by improving the way in which Federal agencies secure their networks. Over the course of a series of hearings, the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, which I chair, learned that agencies were relying on an outdated, expensive, paperwork-heavy systems to secure the technology they rely on to serve the public and protect the important data they are entrusted with. Nobody could say for sure that the system worked and that our agencies were safe from cyber attack. My legislation aimed to hold agencies accountable for continuously monitoring their networks to ensure that they are as secure as possible at all times.

Last year, Mr. Chairman, I was pleased to join with you and Senator Collins in developing comprehensive cybersecurity legislation that would have better secured agency networks while also beginning the process of working with the private sector to secure the critical systems that they own. We introduced what I think as an improved version of our bill again this year.

As my colleagues are aware, it has proven difficult so far this year to find bipartisan consensus on many issues here in the Senate. I have a feeling, though, that it might just be possible in this instance to work across the aisle, like we did after September 11, 2001, to address the serious security challenges that we face as a country. It is my hope, however, that we can act this time before the damage is done.

Thank you. It is great to be here with both of you and we look forward to hearing from our witnesses.

Chairman LIEBERMAN. Thanks, Senator Carper.

Let me just stress something you said. A while back, Senator Reid and Senator McConnell called in the chairs of the six committees with jurisdiction over some aspect of cybersecurity and the Ranking Republican members. It is a sad fact of life around here that I cannot remember the last time that happened. But it also, in this regard, shows how seriously the bipartisan leadership of the Senate takes the cybersecurity challenge. And though there are dif-

ferences that may, in at least one case, fall on partisan lines, this is not a partisan debate. It is a national security debate. And it is an economic growth and security debate. I am confident we are going to go at it with national interests first and partisan interests way behind.

Mr. Reitinger, welcome. This could be the last time you come before us as a witness, so we are probably going to be especially brutal in our cross examination. But, truthfully, thanks for all you have done and we welcome your testimony now.

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

Mr. REITINGER. Thank you very much, Chairman Lieberman, Ranking Member Collins, and Senator Carper, for your leadership on this issue.

The bipartisan approach and the leadership this Committee has shown on this issue has been inspiring to me and the many people I work with, and I would like to thank you, as you thanked me for my efforts, for your efforts to keep this issue on the front burner and to move forward.

Clearly, where you stand depends on where you sit, and I sit in cybersecurity. I would agree with all three of you that there is no more important issue that we need to address in the immediate future than that of cybersecurity. Clearly, the threats are real and they are growing. The hackers are getting better and better and better day to day, and we are depending more and more on the infrastructure which they are attacking every day. This makes our risk profile more and more significant.

It is an issue of intellectual property. Our intellectual property is being stolen. It is an issue of identity theft and our personal information being stolen. But it is much more than that. It is a national security issue. Can we deploy our assets to defend our country? It is a homeland security issue. When you call 911, do people show up? And it is an issue of critical infrastructure protection, not just, again, are our assets taken, but is the power on? Are the phone systems working? Do we have the services we need to operate as a country? No other issue, to my mind, ties together the need for economic success, for economic security, for national security, and homeland security like this issue.

This is a place where we must move forward and we must focus on outcomes. How do we ensure that government has the authorities and the processes and the private sector is moving forward in the right way to jointly advance this issue?

So given the leadership that this Committee has shown, including the work that was done by it in the past Congress, the Administration worked long and hard to put together a legislative proposal which we transmitted to Congress a couple of weeks ago. Certainly, it is a broad issue, but one that does not cover all of the subjects that had been under discussion on the Hill, and we recognize that. So it is the Administration's input into the discussion

[1] The joint prepared statement of Mr. Reitinger, Mr. Butler, Mr. Schwatz, and Mr. Chipman appears in the Appendix on page 40.

and not a bill that we expect the Congress to pass without discussion. We look forward strongly to the discussions that we will have with the Members of this Committee and with the Senate and the House, generally, to make sure that we all move forward in a bipartisan way.

And I cannot emphasize, as a number of the Senators did, the importance of approaching this in a bipartisan way going forward. Cybersecurity cuts across these issues. The Administration's approach over time has not been to say the work of the past Administration was wrong. Therefore, we are going to go in a different direction. Instead, we have tried to take the Comprehensive National Cybersecurity Initiative, which began in the Bush Administration, and continue to advance its efforts and enhance them so that we could move forward as a Nation.

So this proposal does a number of things. It is divided into three main categories: Protecting the American people, protecting government systems, and protecting critical infrastructure. I am going to talk about some of the proposals in those last two categories rather briefly and then I am happy to explore them in the question and answer session.

Within the protecting of the critical infrastructure, one of the things that the bill does, as the Senator indicated, is it gives DHS much clearer authority and responsibility to work in a voluntary way with the private sector. The government does not have all of the answers, but it has some of the answers and it can help the private sector. And so it gives DHS the mission and authorities to help the private sector.

It, as the Chairman indicated, speeds information sharing so that we can get much better data much more rapidly from the private sector so we can have real situational awareness, a real national common operating picture of what the threats look like.

And it, as was discussed in the opening statements of the Senators, creates a framework very similar in many ways to that which the Committee included in its bill that would bring private sector efforts to bear, provide benefits to the private sector companies that identify a set of risks, cybersecurity risks to be identified by DHS, as in the Lieberman-Collins-Carper proposal that came up in the last Congress, with some differences, but a very similar approach.

With regard to protecting the government, the bill does a number of things. It takes a number of the proposals, that Senator Carper has been in the lead in advancing, in modernizing FISMA, taking the ongoing work that has been moving forward to move policy, operational, and oversight mechanisms from the Office of Management and Budget (OMB) to the Department of Homeland Security so we could unite all of those things and then have the capability to observe in real time by continuously monitoring agency networks, as it has been called for, focus on outcomes, and when problems arise, respond to them in real time. Change policy, change oversight, change mechanisms, creating that center of gravity that the Chairman referred to, to much more aggressively protect Federal networks under the Federal Information Security Management Act.

It strengthens DHS's role to deploy more rapidly intrusion protection, intrusion prevention, and other mechanisms for the Federal Government, for example, resolving some of the legal questions that have slowed the deployment of EINSTEIN 2 and EINSTEIN 3 systems. We are continuing to move forward aggressively to deploy them, but the more rapidly we can do that, the better. And it gives DHS, recognizing our similar role to the Department of Defense with regard to Federal civilian networks, similar authorities with regard to personnel, so we could hire people and bring them on board as rapidly as they can in the Department of Defense.

In conclusion, I would simply like to say, in reference to your comments, Chairman, I wanted to offer my thanks to this Committee. I have been with the Department a little over 2 years and it has been one of the best experiences of my life. It has been a real opportunity to serve my country. As I said at the start, I have found the work of this Committee and the focus that you have brought to the issue inspiring to me and inspiring to the entire team I have, including a number of people who are seated behind me, such as Assistant Secretary Greg Schaffer, who will be the Acting Deputy Under Secretary when I depart.

Thank you very much for your leadership of this issue. I look forward to continuing to work with you in whatever new role comes to me. Thank you.

Chairman LIEBERMAN. Thank you very much.

We will go now to Robert Butler, Deputy Assistant Secretary of Defense for Cyber Policy. Thanks for being here.

TESTIMONY OF ROBERT J. BUTLER,[1] DEPUTY ASSISTANT SECRETARY FOR CYBER POLICY, U.S. DEPARTMENT OF DEFENSE

Mr. BUTLER. Thank you, Chairman Lieberman, Senator Collins, and Senator Carper. It truly is a distinct honor and privilege to be before you today. From the Department of Defense's perspective, as has been discussed, we focus first and initially on the threat, a threat that continues to grow against our critical information systems that comes from nation states, terrorists, criminal organizations, and malicious hackers.

DOD is reliant, as you know, on the Nation's critical infrastructure, whether we are talking about deployment or employment of forces. We are critically dependent on power generation, all modes of the transportation sector, telecommunications, of course, and the defense industrial base to perform the missions that we have been assigned as well as are expected to do overseas.

Just as our reliance on critical infrastructure has grown, so, too, have the threats that we are facing today. Probably the most perplexing concern is the asymmetric threats, the threats that continue to advance in sophistication and in persistence. And so it is not just about intellectual property theft today, but the real possibility of a large-scale attack on any segment of America's critical infrastructure that would be disruptive to our way of life.

[1] The joint prepared statement of Mr. Reitinger, Mr. Butler, Mr. Schwatz, and Mr. Chipman appears in the Appendix on page 40.

I believe that fact has been recognized and encouraged discussion on the matter of what we are about to deal with today. And, in fact, as the President has stated, the status quo is really no longer acceptable, not when there is so much at stake and we can and must do better.

The most important aspect from DOD's perspective as we look at the Nation's critical infrastructure and what to do about it is really that it is not dependent upon any particular entity or party. It really requires a whole of government and really a whole of America approach, necessitating many different Federal agencies, State governments, and the private sector to work together.

This proposed legislation is an important step in that direction. It breaks down the barriers to information sharing so that stakeholders can really communicate effectively. It updates the criminal statutes, such as the Racketeering, Influenced, and Corrupt Organizations Act, to deter criminal activity. It engages the private sector as valuable stakeholders and really strengthens the ability of the Department of Homeland Security to lead the Executive Branch in defending the Nation against this threat. As Mr. Reitinger has explained, it really advances us not only in FISMA, but in other provisions, especially in growing the next generation workforce and hiring practices and exchange of personnel. Importantly, this legislation accomplishes all of this while respecting the values of freedom and ensuring the protection of privacy and civil liberties that we cherish so deeply in our country.

The Department of Defense has an important role, as you know, in protecting the military networks and the national security systems while providing support and technical capabilities to help protect other critical infrastructure. DOD has and will continue to work hand-in-hand with the departments alongside of us here at this table as well as the other Departments within the Executive Branch and with the private sector, in countering cyber threats and protecting our national critical infrastructure. We really look forward to the leadership that this Committee has taken and working with Congress to make sure the Executive Branch has the appropriate authorities for cybersecurity and improving the overall security and safety of our Nation. Thank you.

Chairman LIEBERMAN. Thank you, Mr. Butler. I appreciate that you are here.

Next, we will go to a familiar face at the Committee, Ari Schwartz, who is here before us today as the Senior Internet Policy Advisor at the National Institute of Standards and Technology (NIST) at the Department of Commerce. Thank you for being here.

TESTIMONY OF ARI SCHWARTZ,[1] SENIOR INTERNET POLICY ADVISOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. SCHWARTZ. Thank you, Mr. Chairman. It is good to be back. Ranking Member Collins, Senator Carper, and Mr. Chairman, it is a pleasure to be here and thank you for inviting me to testify on behalf of the Department of Commerce and the National Institute

[1] The joint prepared statement of Mr. Reitinger, Mr. Butler, Mr. Schwatz, and Mr. Chipman appears in the Appendix on page 40.

of Standards and Technology on the Administration's cybersecurity legislative proposal.

The main goal of the proposal is really to maximize the country's effectiveness in protecting the security of key critical infrastructure networks and systems that rely on the Internet, while also minimizing the regulatory burden on the entities that it covers and protecting the privacy and civil liberties of the public—quite a tall order.

I will be addressing five important pieces of the proposal. The first is creating the security plans, as Senator Collins discussed in detail. Second is promoting secure data centers. Third is protecting Federal systems. Fourth, data breach reporting. And fifth, privacy protections.

An important theme of the proposal is accountability through disclosure. In requiring creation of security plans, the Administration is promoting the use of private sector expertise and innovation over top-down regulation. Importantly, the proposal only covers the core critical infrastructure as it relates to cybersecurity. DHS would define these sectors through an open public rulemaking process. The critical infrastructure entities will take the lead in developing frameworks of performance standards for mitigating identified cybersecurity risks and could ask the National Institute of Standards and Technology to work with them to help create cybersecurity frameworks.

There will be strong incentive for both industry to build effective frameworks and for DHS to approve those created by industry. The entities involved will want the certainty of knowing that their approach has been approved, and DHS will benefit from knowing that it will not need to invest the resource-intensive approach of developing a government-mandated framework unless industry really fails to act. Covered critical infrastructure firms and their executives will have to sign off on the cybersecurity plans, subject them to performance evaluation, and disclose them in their annual reports.

Rather than substituting the government's judgment for private firms, the plan holds the covered entities accountable to consumers in the market. This encourages innovation in mitigation strategies as well as improving adherence to best practice by facilitating greater transparency, understanding, and collaboration. The main goal is to create an institutional culture in which cybersecurity is part of everyday practice without creating a slow-moving regulatory structure.

In that same spirit, the Administration also seeks to promote cloud services that can provide more efficient services and better security to government agencies and a wide range of businesses, particularly small business. To do so, the draft legislation proposes to prevent States from requiring companies to build data centers in that State, except where expressly authorized by Federal law.

The proposal also clarifies roles and responsibilities for setting Federal information security standards. Importantly, the Secretary of Commerce will maintain the responsibility for promulgating standards and guidelines, which will continue to be developed by NIST. DHS will use these standards as a basis for the binding directive and memoranda issued to Federal agencies. A working part-

nership between Commerce, NIST, and DHS will be essential to ensure that agencies receive information security requirements that are developed with the appropriate technical, operational, and policy expertise.

On data breach reporting, as my colleague from the Department of Justice (DOJ) will detail, the Administration has learned a good deal from the States, selecting and augmenting those strategies and practices we felt most effective to protect both security and privacy. The legislation will help build certainty and trust in the marketplace by making it easier for consumers to understand the breach notices that they receive and why they are receiving them. As a result, they will better be able to take appropriate action.

As Secretary Gary Locke and others at the Commerce Department have heard from many companies in different industries, including in response to our Notice of Inquiry on the topic last year, a nationwide standard for data breach notification will make compliance much easier for the wide range of companies that must follow 47 different legal standards today.

Finally, I would like to point out that many of the new and augmented authorities in this package are governed by a new privacy framework for government that we believe would enhance privacy protection for information collected and shared with government for cybersecurity purposes. This framework would be created by DHS in consultation with privacy and civil liberty experts and the Attorney General, subject to regular reports by the Justice Privacy Office, and overseen by the independent Privacy and Civil Liberties Oversight Board. Government violations of this framework will be subject to both criminal and financial penalties.

Thank you again for holding this important hearing, and thank you for your leadership on this issue. I look forward to your questions.

Chairman LIEBERMAN. Thanks, Mr. Schwartz. As I bid farewell to Mr. Reitinger, I should have formally welcome you to government service.

Mr. SCHWARTZ. Thank you.

Chairman LIEBERMAN. You appeared before us many times in your independent advocacy role.

The final expert on the panel will be Jason Chipman, Senior Counsel to the Deputy Attorney General, Department of Justice. We now look forward to your testimony.

TESTIMONY OF JASON C. CHIPMAN,[1] SENIOR COUNSEL TO THE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. CHIPMAN. Thank you, Chairman Lieberman, Ranking Member Collins, and Senator Carper. It is a real pleasure to be here and I appreciate the opportunity to testify on behalf of the Department of Justice about the Administration's cyber legislative proposal.

This Committee knows well that the United States confronts a serious and complex cybersecurity threat. The critical infrastruc-

[1] The joint prepared statement of Mr. Reitinger, Mr. Butler, Mr. Schwatz, and Mr. Chipman appears in the Appendix on page 40.

ture of our Nation is vulnerable to cyber intrusions that could damage vital national resources and put lives at risk. Indeed, intruders have stolen confidential information, intellectual property, and substantial amounts of money.

At the Department of Justice, we see cyber crime on the rise, with criminal syndicates operating around the globe with increasing sophistication to steal from innocent Americans. Even more alarming, these intrusions might be creating future access points through which criminal actors and other adversaries can compromise critical systems during a crisis or for other nefarious purposes.

President Obama has stated publicly that cyber threats represent one of the great challenges to the economic and national security of our country. Indeed, given the scope of the problem, as you have heard and as you know, the President has made this a significant priority for the Administration.

Over the past few years, all of the agencies before you have made great progress in confronting these threats. At the Justice Department, our criminal and national security investigators and prosecutors and attorneys have been working hard establishing new units, like the National Cyber Investigative Joint Task Force, to pull together the resources of many different agencies to investigate and address cybersecurity threats.

With that said and despite good work in this area, the problem is far from resolved. It is clear that new legislation can help tremendously to improve cybersecurity in a number of critical respects.

From the Justice Department's perspective, I would like to take a moment to highlight two parts of the Administration's cyber legislative package aimed at confronting identity theft and at improving the tools that we use to fight computer crimes.

First, the Administration's proposal includes a new national data breach reporting requirement. Data breaches frequently involve the compromise of sensitive personal information that subject individual consumers and citizens to identity theft or to other crimes. Right now, as Mr. Schwartz mentioned, there are 47 different State laws that apply in different situations and require reporting through different mechanisms. The Administration's data breach proposal would replace those 47 State laws with a single national standard applicable to companies and institutions that meet a minimum threshold set forward in the draft bill. If enacted into law, this proposal would ensure that companies notify consumers when sensitive personal information is stolen or compromised, and it would require that they give them information about what they can do in response to the theft or the compromise of their information.

The proposal would empower the Federal Trade Commission to enforce the reporting requirements and it would establish new requirements for what must be reported to law enforcement agencies when there is a significant intrusion so that institutions like the FBI and the U.S. Secret Service can quickly work to try to identify the culprits and protect others from being victimized. We believe that the national standard would also make compliance easier for industry, which currently has the burden of operating under a patchwork of different rules.

Second, the Administration's proposal includes a handful of changes to the criminal laws aimed at ensuring that computer crimes and cyber intrusions can be investigated and punished to the same extent as other similar criminal activity. Of particular note, the Administration's proposal would clearly make it unlawful to damage or shut down a computer system that manages or controls critical infrastructure, and it would establish minimum sentence requirements for such activities. We believe this narrow, focused proposal will provide strong deterrence to this class of serious and sometimes potentially life-threatening crimes.

Moreover, because cyber crime has become a big business for organized crime groups, the Administration proposal would make it clear that the Racketeering, Influenced, and Corrupt Organizations Act (RICO), applies to computer crimes.

Also the proposal would harmonize the sentences and penalties for violations of the Computer Fraud and Abuse Act. For example, acts of wire fraud in the United States carry a maximum penalty of 20 years in prison, but similar violations of the Criminal Fraud and Abuse Act very frequently carry a maximum of 5 years in prison. That is a discrepancy we think should be corrected.

Mr. Chairman and Members of the Committee, this is an important topic. The country is at risk. There is a lot of work to be done to protect the critical infrastructure of our country and to stop computer crimes from victimizing and threatening Americans. I look forward to answering your questions. Thank you very much.

Chairman LIEBERMAN. Thanks, Mr. Chipman.

You know, the testimony of the four of you makes clear how comprehensive the President's proposal is, of course, as is the Committee's proposal. I think both are necessarily comprehensive administrative reorganizations to better deal with the security threat, both also involve questions of how we protect civil liberties, privacy, and then what the role of the law is here. Are there not certain kinds of behavior in cyberspace that ought to be officially designated as illegal, adjusting existing legal framework. So the testimony has been very helpful.

We will do a first round of 7 minutes each.

Mr. Butler, let me begin with you because in the discussion of cybersecurity, both inside Congress and outside, and various times, people have said, look, the expertise in this area and in our government is in the Department of Defense and the National Security Agency (NSA). Maybe DHS is not the right place to be given enhanced authorities, but I take it from your testimony and the process that was going on within the Administration that a decision has been made which is supported by the Department of Defense that when it comes to the dot-gov, that is, the non-Defense dot-gov and dot-com networks, that it is the Department of Homeland Security that should have primary responsibility. Is that right?

Mr. BUTLER. That is correct, Mr. Chairman. If you have watched the Department of Defense and the Department of Homeland Security dialogue over the last couple of years, it really has grown in the areas of collaboration. Probably one of the hallmark events was last year's signing of a Memorandum of Agreement (MOA) between Secretary Janet Napolitano and Secretary Robert Gates which laid

out a foundation for new ways of collaborating as we move forward in operational planning as well as in capability development.

So the sharing of technical expertise from the National Security Agency, being an element of that, the formation of a joint coordination element up at Fort Meade led by a DHS senior as part of that, the sharing of personnel between the two departments in different ways that allows a better understanding of not only capabilities but how to best satisfy information requirements, while at the same time ensuring strong oversight of privacy and civil liberties by having DHS very much engaged with the Department of Defense on looking at those issues.

So over the last year, especially, I think we have seen new ways of doing business together, certainly from Secretary Gates' perspective and the Department's perspective, and the recognition that DHS is the leader with regards to cyber protection for our Nation. We are now working towards a unifying vision for how we will protect and help enable the protection of not just dot-gov and dot-com, but working to learn from what we have experienced on the dot-mil side, as well.

Chairman LIEBERMAN. So thank you. You actually answered my second question before I asked it, which was what are we doing to make sure that the Department of Homeland Security in some sense leverages on the expertise that DOD and NSA have rather than recreating them within the Department of Homeland Security.

Mr. BUTLER. So a key element of that was an agreement between the two Secretaries that we would, one, share personnel. Two is to actually develop a set of activities underneath the joint coordination element to really help us understand how we could better leverage what is in the Department of Defense today. I think a good example of that is the work being done to help with the National Cyber Incident Response Plan. And then going beyond that, looking at other efforts where we can share both in capability expertise as well as in technology what we are doing with intrusion detection and intrusion prevention systems as we move forward in time, so the EINSTEIN 3 efforts can move forward.

Chairman LIEBERMAN. Mr. Reitinger, from a DHS perspective, how would you evaluate the relationship between your Department and DOD? Obviously, part of what you have wanted to do is build up your own expertise within DHS, but also, as I said, to leverage on what already exists in DOD and NSA.

Mr. REITINGER. Thank you, Chairman. That is exactly correct. I think we each bring unique things to the table. Certainly, DOD has unparalleled technical expertise and cybersecurity expertise build up over the course of years. In the Department of Homeland Security, we have built up our own expertise, particularly around things like control systems, how to work broadly across a broad distributed interagency and deal with the multiple barriers that one faces in that space.

As a result, I think over the course of the last year, as Mr. Butler indicated—we are very good friends—we have built up a much stronger partnership, not only having the MOA, which along with that joint coordination element works to make sure that we can stay fully operationally synced with DOD on a very tight basis. We

will be developing people that will be deployed in the NSA Technology and Acquisitions Directorate so that as it develops technology, it meets Homeland Security needs, as well. We will be deploying people in the Threat Operations Center at NSA so we have full knowledge of what they are seeing from a threat perspective. And similarly, both Cyber Command and the National Security Agency will deploy elements to the National Cybersecurity Communications and Integration Center to support our operations under the National Cyber Incident Response Plan. So from Cyber Command, there will be a cyber support element, a team of people at our offices on Glebe Road, and a cryptologic support group from NSA, to similarly support what we do.

But separate and apart from the MOA, we continue to work together. We literally meet regularly with DOD at the deputies' level to make sure that we can stay fully synced at a leadership level, and Mr. Butler and I personally participate in a weekly secure video teleconference with individuals from NSA and other people from DOD and DHS so that we do not allow any delta to occur in terms of what our operational activity is so we can move together most effectively.

Chairman LIEBERMAN. That is great to hear. That is exactly the opposite of the kind of stovepiping that we always worry about, and obviously it is critically necessary.

Mr. Butler, did you want to add anything?

Mr. BUTLER. Just one additional element. Building beyond the National Security Agency, we have found ways to better collaborate with the Defense Cyber Crimes Center. So as was mentioned, cyber crime is a big issue. We are working with DHS now, looking at how we can leverage forensics expertise to help not only with the defense industrial base, but helping in other parts of the critical infrastructure that we are trying to protect.

Chairman LIEBERMAN. Mr. Schwartz, just building a little bit on your previous existence as an advocate for privacy, is it correct to assume, just to build on the record here, that if the Committee and the Administration came in with a proposal that put responsibility for the dot-com and dot-gov, particularly dot-com cyberspace into the Department of Defense and NSA, there would be real concerns in the privacy community?

Mr. SCHWARTZ. I think that if you were to take the core critical infrastructure and put that regulatory authority primarily at the Defense Department, there would be major concerns from privacy and civil liberties groups.

Chairman LIEBERMAN. Thank you. Mr. Reitinger, this Committee in its broad homeland security responsibility often interacts with the private sector, and when we come to a question of how we protect infrastructure, we have become accustomed to saying that 85 percent of the infrastructure of the United States is owned and operated by the private sector. What would you say that percentage is for cyberspace, if you can hazard a guess, and I am not going to hold you to this.

Mr. REITINGER. Sir, I have heard everything from 75 to 95.

Chairman LIEBERMAN. Yes.

Mr. REITINGER. I will freely admit to you, I have never seen a rigorous analysis of this.

Chairman LIEBERMAN. Right.

Mr. REITINGER. I think it varies from country to country. Certainly, in the United States, it is the vast majority, and even when you talk about government critical infrastructure, in many cases, it is the State and local government critical infrastructure that is often more important on a real-time basis than the Federal critical infrastructure. So we absolutely need to work closely with our critical infrastructure partners, our State, local, tribal, and territorial partners, and our Federal Government partners to secure critical infrastructure.

Chairman LIEBERMAN. So, bottom line, whatever the exact percentage, it is clear from what you said that there is a consensus that most of cyberspace is owned or operated by the private sector, and that makes the parts of this legislation that create and authorize new ways for the Department of Homeland Security to interact with the private cyberspace infrastructure, particularly with regard to the dot-com networks, critically important.

My time is up on this round, but I will come back to that after my colleagues have the next round. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Reitinger, about a year ago, you testified before our Committee that Section 706 of the 1934 Communications Act already provided emergency authority to the President. That prompted me to actually go read Section 706 of the 1934 Communications Act, and I am not going to read all of it out loud today, but let me just read parts of it, because I think that it will emphasize two points. One, that the President's authority under this law is enormously broad, and second, that the language shows that it was written for another era.

The section says that when the President finds that there is war or a threat of war or a state of public peril or a disaster or any other national emergency, that the President may cause the closing of any station for radio communication. The President may remove all the equipment and apparatus from the station. He may authorize the use and the control of the station by any department of government. In other words, under this section of the law, the President is allowed to have the government actually take over any radio station in the United States, or close it down completely, or remove the equipment from it.

Nowadays, if that were proposed, it would create a tremendous uproar and free speech concerns. This authority is far broader than the authority in our bill, since this authority does allow a government takeover of transmission equipment, and it is clearly outdated since it is tied to traditional communication facilities and it does not reach interconnected critical infrastructure entities that are not covered by the Communications Act.

We spent a lot of time, and indeed, most recently revised our bill to carefully constrain and define exactly what authority the President would have. We made it very clear that the President could not shut down the Internet, that government could not take over the Internet. There was a lot of theories in the Internet world that perhaps we wanted that. We did not, but we made it explicit in our new bill. We carefully constrained the President's authority with

reporting to Congress, with time limits, with privacy limitations, by saying it has to be the least intrusive means possible.

So I am very curious why the Administration, in your approach, does not update the 1934 Communications Act, which clearly speaks to a different era, and carefully define exactly what the President's authority would be. And Mr. Chipman, just to put you on notice, since you are from the Justice Department, I am going to ask you that question, as well.

Mr. REITINGER. So, thank you, ma'am. I will do my best. You are clearly correct. Let me agree with you that the statutory authorities that exist in this space were written long ago, as you said, in 1934, and were not designed with the current environment that we have in mind. There are authorities there.

That said, the Administration's bill does not include any additional emergency authorities for the President. Instead, as you point out, neither the Committee nor the Administration has sought or seeks any form of Internet kill switch. This is, however, a critical issue. Clearly, if something significant were to happen, the American people would expect us to be able to respond, and respond appropriately.

To that end, we would, if something significant happens, use the authorities that we bring to bear in the right way, not to restrict Internet freedom, but to preserve Internet freedom while protecting the country, and we would do so using the authorities that we currently have and the processes that we have developed, such as the National Cyber Incident Response Plan, which details the roles and responsibilities and how we would move forward to respond to an event.

I can say, as you pointed out, Ranking Member Collins, this is a critical issue. This is an area where I think different people have different views about how the government ought to be empowered and what the constraints on the government exercise of authorities ought to be. And this is a key area where I would hope there would be further discussions between the Administration and the Congress to figure out the right set of mechanisms, if any, that were necessary to move forward in this space.

Senator COLLINS. Mr. Chipman, you represent the Justice Department. Why did the Justice Department not recommend amendments to the 1934 Communications Act, which is clearly outmoded, and also a carefully constrained limitation, carefully defined, on what the President could and could not do if there was a cyber emergency?

Mr. CHIPMAN. Thank you. Senator, I think I would echo Mr. Reitinger's comments and say that, clearly, this is an important topic, and clearly, it is an issue that merits discussion, and I think it is fair to say the Administration wants to engage in that discussion with you and your colleagues.

In my experience, the issue of what emergency powers are needed tends to be very context-driven, and so the answer to that question, I think, becomes fairly nuanced depending on what type of emergency the government is facing. I think, no doubt, Mr. Reitinger is quite right. The American people expect the government to be able to respond, and I think that the work DHS has done within the interagency to create a National Cyber Incident

Response Plan is quite key. But beyond that, in terms of the specifics of this particular Act, I think it merits discussion, but it is not in the Administration's proposal right now.

Senator COLLINS. But that perplexes me. This is an area where we should be thinking ahead about exactly what authorities we want the President to have rather than leaving it ambiguous, rather than relying on a 1934 law that allows the President to take over control of radio stations. This just does not make sense to me and I hope you will work further with us to carefully define what the authorities are and to update the law.

Let me just make one other quick comment, since my time has expired. I cannot help but be struck by the irony that we have four different departments represented here today, and that is a very good thing because it shows that the Administration is working across departments. But it is ironic, because unlike our bill, the Administration chose not to include in its bill an entity similar to the National Counterterrorism Center which would bring together within DHS representatives of all of your agencies as well as the Director of National Intelligence and other agencies so we would institutionalize the kind of coordination and cooperation that you have described is occurring informally. So it is ironic that the Administration has four departments represented here, yet has rejected the construct that we have in our bill of institutionalizing that interagency cooperation.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

For the record, I share Senator Collins' sense of irony about this, truly. Also, for the record, I do think the country would be better off if we did create some new law regarding the authority of the President to act in these emergencies. As Senator Collins and I know, this can be a very controversial area because people can quite easily misunderstand. There is an admirably ferocious interest among inhabitants of cyberspace in their privacy and liberty. You know, God bless them, I agree, and so we want to hear that voice. But in the case of a really catastrophic emergency, I think we want to be clear that the President has authority to act, and frankly, in a way that the 1934 law does not make clear, that there are limits to what we want the President to do and that does require new statutes. So I pick you up, Mr. Reitinger, on your suggestion that this is an area where we should, in the best Biblical sense, reason together.

Senator Carper.

Senator CARPER. Thanks very much.

Mr. Reitinger, as you prepare to depart, any final words of advice? Let me just ask, first, what do you feel especially good about that has been accomplished during your watch, and what are some of the areas that you think we have some serious work still to do?

Mr. REITINGER. Well, thank you, sir. It is rare to have the opportunity to say something like that, so let me just say a couple of things. I feel most happy about two things. One, the fact, as was just remarked by the Chairman and the Ranking Member, that we have four departments and agencies up here all speaking from the same voice. The fact that we have a cross-government approach, and indeed, an approach with many people in the private sector,

as well, that says, here is how we think we need to move forward as a Nation. One can agree or disagree with what that approach says, but that we are collaborating effectively under the leadership of Howard Schmidt at the White House and broadly across agencies, I think, is a very positive thing.

The other thing I would say I am most happy about is the team that we have built at DHS. The fact that, going back into the prior Administration—at one point about 3 years ago, DHS had about 40 people working in cybersecurity. We are up to about 260 now and we will be growing towards 400 by the end of fiscal year 2012. So we have built a significant team with significant capabilities that brings a lot to the table, some significant expertise, and can leverage other sources of expertise in government, including DOD, the Department of Commerce, and the Department of Justice. So the people piece that we have built, both across government and with the private sector and within DHS, is the thing that I am most proud of because I believe that organizations and entities succeed or fail based on the people, and so that is what is most important to me, sir.

Senator CARPER. And maybe in the category of incomplete, what are some major to do's that are still out there for whoever succeeds you and the rest of us?

Mr. REITINGER. Sir, there are innumerable to do's. It is an old saying, but a true one, to say cybersecurity is a journey and not a destination. As we get better and better, so will the bad guys. I can say that as a former prosecutor. They continue to share information, to develop new techniques, and so this is not a game that we are going to win. This is a game we are going to do better at and win more often, but it is not going to end.

So the major thing to do that unites all of those things together is the need to keep focus on this issue, to make sure that it stays on the front burner, and to make sure that Congress and the Administration and the private sector work together to pass cybersecurity legislation as rapidly as possible.

Before and after that legislation is passed, we need to make sure that we are doing the right things, both in implementation of measures, in development of strategy, and in hiring of people broadly across the public and private sectors that ensure that cybersecurity retains the level of importance that we have given it very broadly across the homeland security enterprise and the national security enterprise.

One of the things that I like to point out is that a little over a year ago, on February 1 of last year, the Department of Defense and the Department of Homeland Security released their Quadrennial Strategies, on the same day, and in the Quadrennial Defense Review, cybersecurity received a new and increased level of importance for the Department of Defense.

Similarly, in the first ever Quadrennial Homeland Security Review, cybersecurity rose to one of the top five mission areas of the entire homeland security enterprise, and that is not just DHS. That includes the private sector and multiple government agencies.

So we have got the right focus on the issue. We have the right importance. It has to stay there.

Senator CARPER. Well, my guess is the media will help us with that, because every time there is one of these disclosures, we hear a lot about it, and that is probably not a bad thing.

Just to follow up on the question I have asked you, how have things improved in recent months under the reforms that have been put in place under current law, and maybe give us some other ideas about how this proposal would further improve things.

Mr. REITINGER. Certainly, sir. So we have been staffing up, as your question indicates, over the past year-plus a lot of the things that are described in the Federal Information Security Management Act reforms. We have been taking significant steps to implement under administrative processes. So in two memoranda, I believe M–10–15 and M–10–28—it is sad that I might remember this——

Senator CARPER. That is sad.

Mr. REITINGER. It is, sir. [Laughter.]

Senator CARPER. But I am glad at least someone is remembering that.

Mr. REITINGER. I am working on this. I will work to forget them by mid-summer.

Senator CARPER. The next time I see you, I will say, what were those numbers? [Laughter.]

Mr. REITINGER. OMB, sir, has been working, one, to move more and more towards continuous monitoring, and two, to transfer a lot of the operational responsibilities for FISMA to DHS. So we have been building up the capabilities. We have been working with the Department of Justice, in particular, to expand and roll out CyberScope, which is an online continuous monitoring tool that will be used to work more directly with the agencies, for example, holding deeper dives on agency security. It is what we call the CyberStat process, with the collaboration and work with OMB.

So we have been working to roll out that greater focus, and again, in full partnership with the Department of Commerce, who has the lead on the development of standards for the Federal Information Security Management Act, to work together to deploy a focus on continuous monitoring, on real-time metrics, and we are going to continue that process, which will, in fact, accelerate if an appropriate FISMA reform act is passed.

Senator CARPER. All right. Thanks. Mr. Reitinger spoke proudly of the Department's ability to attract and put together a good team and still attract more, hopefully well-qualified people. But the question I have of the panel, in order to have effective cybersecurity both in government and in the private sector, we are going to need to attract a significant number of additional qualified people with the same skills as those who are seeking to do us harm. Let me just ask, what kind of job do you think we have done to date in finding those people, not just in the Department, but outside of the Department, and not just in government, but outside of government? Do we need to give agencies more tools to hire the right people and retain them once they are here? Mr. Butler.

Mr. BUTLER. Thank you, Senator Carper.

I will speak from a DOD perspective as well as from being in this business for a while, both on the private sector and public sector side of the house. Importantly for the Department of Defense, it is

not only about today, but it is about tomorrow and the next generation workforce. And so Secretary Gates has made it a big priority.

As we work through a variety of what I would call pilot initiatives—Cyber Patriot at the high school level, State competitions, National Defense Cyber Competition, I mentioned the Defense Cyber Crimes Center and its National Digital Forensics Competition—we are building not only competitions, but mentoring and coaching programs. Those mentoring and coaching programs really become, I think, the heart and soul of what we need to recruit from both a national security base and a homeland security base. Whether those individuals go into the private or public sector, we are seeing both an aptitude and an attitude about cybersecurity.

I spoke for the Deputy Secretary of Defense at the Cyber Patriot Competition, which was held about a month ago, the national competition, and we are now not just pulling from military institutions and high schools and colleges, but really now creating a base that is allowing us to go across the country into the inner cities to inspire kids for the next level.

We are working through, I think, with limited funding, different ways to incentivize that and to continue those programs. But to me, those are the important elements that we need to——

Senator CARPER. Good. That is very helpful. I am out of time. Mr. Schwartz, just very briefly, and then Mr. Chipman, if we could do that.

Chairman LIEBERMAN. Yes.

Senator CARPER. Go ahead.

Mr. SCHWARTZ. I will say I have been in the government for 9 months at NIST and I have been really impressed with the folks that we have in NIST. I think part of that is the great environment, but it is also that hiring authority that was mentioned. At NIST, we do have direct hire authority, and we have the flexible hiring. That has given us the ability to hire and compete with others that need those cybersecurity aims. So I completely understand where this Committee has come down in terms of DHS getting similar authorities and that is in the Administration's proposal, as well.

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

Mr. CHIPMAN. Thank you. I would add that I know that this is an important aspect of the Administration's focus on cybersecurity, indeed, the Comprehensive National Cybersecurity Initiative that Mr. Reitinger mentioned included cyber education as a very important topic, and I know that work has continued.

At the DOJ, it is certainly an important topic that is getting a lot of attention, especially at the FBI. I know the FBI in recent years has created a 5- to 7-year training program for agents to make sure that they are equipped to confront the sorts of cyber threats that we have been talking about.

Senator CARPER. All right. Thanks, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper.

Mr. Reitinger, let me come back to the topic I raised at the end of my first round of questions and pose it in this general sense and ask you to answer it in that way, which is since we agree that most of cyberspace is in the hands of the private sector—appropriately, rightly—and we also understand that attacks on privately owned

cyberspace can have very serious effects on our economy and our national security—obviously, we know that some of these are going on right now. So the question is, what is the approach in the White House proposal for making sure, to the best of our ability, that the private sector is taking steps to defend itself, particularly the most critical parts of it, and in that sense to defend our country, because an attack on our privately-owned infrastructure in cyberspace, electric grid, transportation systems, or finance systems could have, in many ways, as devastating an effect as a conventional military attack? So give us an overview of what the approach is in the White House legislation to the private sector.

Mr. REITINGER. Thank you, Mr. Chairman. The approach is actually, I think, as I said before, very similar to that that was in the bill that this Committee developed last year. There are a couple of concerns here. One is that, clearly, cyberspace is not an area that is amenable to extensive top-down prescriptive regulation. The technology moves too quickly. There are innumerable differences between entities. So one needs to find the right way to bring the expertise of the private sector to bear, to continue to rely on innovation to address the problem, and then also to ensure that you have the right mechanisms to ensure that homeland and national security requirements are met.

And it is that last space that, I think on occasion, we have not seen as much progress as we all believe that we should have. We need to find the right way to set requirements in a way that actually reward private sector companies that are doing the right thing, that give a benefit, and make sure that without unduly restricting innovation in any way, that we do make sure that the power stays on, that the most critical of critical infrastructure can continue to operate.

The approach that the Administration took is similar to the one that the Committee developed.

Chairman LIEBERMAN. Right.

Mr. REITINGER. In essence, the Department of Homeland Security, in collaboration with the partners that you see at this table and the private sector, would develop a set of criteria for determining, again, what is the most critical of critical infrastructure. So the notion is that this would not be every part of current critical infrastructure, but absolutely the most important pieces.

Chairman LIEBERMAN. So we start with priorities.

Mr. REITINGER. Yes, sir. We prioritize what has been referred to in the bill as covered critical infrastructure.

Chairman LIEBERMAN. Right.

Mr. REITINGER. And for those entities, DHS would identify—I am going to say this a bunch—again in collaboration with the government agencies you see and in the private sector, a set of risks that would need to be mitigated. So this would not be a, "Thou shalt not use this technology," but here is a risk and you need to have a mechanism to identify it.

And then under the Administration's approach, DHS would not then say, here is a set of choices you have. You have to do one of them. Instead, industry, the private sector, would be responsible for putting forward frameworks of essentially performance standards and/or performance measurements that would focus not just

on particular steps that you need to do, but on actual effectiveness, on measurements that would indicate how effective the measurements were, and then industry would develop a plan. So any covered entity would need to develop a plan that aligned with that framework and was evaluated under that framework for addressing the risk that DHS identified.

Then, industry would also be responsible for having itself evaluated by a set of effectively certified evaluators.

Chairman LIEBERMAN. Right.

Mr. REITINGER. So it would not be DHS doing the direct evaluation, but there would be entities that were chosen to do evaluations. Industry would receive those evaluations and then would publish—so the biggest lever would be transparency. Industry would publish the high-level description of its plan and a high-level description of the evaluation results. And then we would use that transparency to drive market activity that would enhance security in covered critical infrastructure and as a standard of care is developed more broadly throughout critical infrastructure.

In addition, and as an additional incentive, there could be procurement advantages or disadvantages based on how one did in the process——

Chairman LIEBERMAN. Explain that a little bit more. So that is the next point. I think that your description is excellent. You are right. The White House and Committee bills have a generally similar proposal, although as you know, we give DHS the authority to evaluate the plans as opposed to third-party. But is there a reward and punishment here? In other words, do industries that follow their plans get rewarded and ones that do not get, in some sense, punished?

Mr. REITINGER. So, yes, sir. There are a number of different levers, or levels, and I might ask Mr. Schwartz to supplement this, because he has a particular taxonomy that I happen to like. But in essence, one, your evaluation results will be published, so there is a direct ability of the market, your key partners and customers to take that into account.

Second, the activity, the process of developing these frameworks and plans is going to start to create a standard of care that entities will need to step to over time, perhaps for insurance purposes, perhaps for other purposes.

Last, DHS is directed to work with the Federal Acquisition Council so that the results of these evaluations can appropriately be taken into account in Federal procurements, which will provide an additional incentive to private sector players.

It is very much intended to be a light-touch approach, but one that we believe, over time, will move the private sector and critical infrastructure in the right way, will reward the companies that are doing a very good job, and will get us to a more secure state in the future.

With your permission, sir, I would like to ask Mr. Schwartz to supplement that.

Chairman LIEBERMAN. The resident taxonomist.

Mr. SCHWARTZ. Getting to this balance of the right levers and incentives is really the key to answer these questions for covered critical infrastructure as we see it in the plan, and there are a number

of incentives that you have identified in your bill that we have put forward here; most of them are similar. The question is getting at the right particular balance between them.

The taxonomy that Mr. Reitinger is referring to breaks down to four different areas that are somewhat related. One is the effects of public disclosure for cybersecurity performance.

Chairman LIEBERMAN. So a kind of public incentive or shame?

Mr. SCHWARTZ. Well, the second, I would say, is reputation and risk——

Chairman LIEBERMAN. Right.

Mr. SCHWARTZ. It is more that they know that markets may act on it. Where the second is, really, if they do things completely wrong, then you are going to have brand impact, potentially, where markets really exist in that space.

Chairman LIEBERMAN. OK.

Mr. SCHWARTZ. And the third is access to government procurement, so questions about procurement, and our bill links it to the Federal Acquisition Regulation (FAR) and——

Chairman LIEBERMAN. In other words, you can make some more money. You will have preference in selling, or offering services to the government.

Mr. SCHWARTZ. Correct. And the fourth is perceived litigation risk that shareholders or others may come forward with, and that would have to work out over time, as well.

But we are open, and we do not claim to have everything in perfect alignment or balance in terms of these levers. No one can know exactly what will happen in terms of getting this right, but we can work together with you to try and come up with what we think is the best solution. So we are completely open to having this discussion about what are the best incentives moving forward.

Chairman LIEBERMAN. Good. No, that is very helpful, because our bill, as you know, has a provision for limited liability protection as another incentive, consistent with the Administration approach to the private sector to take preventive, defensive action so that, in one case, if they did, they would be protected, for instance, from punitive damages and liability.

In the extreme case of a President taking action in a catastrophic case, whether under the old law or under our proposal, to protect really the national interests, there would probably be claims, significant ones, against some elements of the cyberspace community, and the question there that we raise is whether they ought to be protected from liability overall because they were acting pursuant to an order of the President of the United States.

Do either of you want to comment on the general subject of offering some liability protection to the private sector as an additional incentive beyond what the White House proposes to the private sector to cooperate?

Mr. REITINGER. I think I would simply say two things, Mr. Chairman. One, as Mr. Schwartz indicated, and maybe I will call that the Schwartz taxonomy—the balance—there's different ways to tweak it, and I think we would be happy to continue to discuss that with you.

Second, there is some liability protections, not under this particular provision dealing with the overall incentives regime for the

private sector, but to the extent that the private sector shares information with government or is assisting government with protecting dot-gov, there is both an immunity and a good faith immunity that is written into that section of the statute.

Chairman LIEBERMAN. Do you want to add anything, Mr. Schwartz?

Mr. SCHWARTZ. I will just say, it is similar to my comments about being open to the levers——

Chairman LIEBERMAN. Yes.

Mr. SCHWARTZ [continuing]. That we are definitely interested in having this discussion with you to further figure out how we can come up with the right balance here, and this fits into that discussion.

Chairman LIEBERMAN. This could, unfortunately, end up as a real obstacle to the passage of the bill, the failure to do something about liability, and I think it would be good if we worked together to try to find a common ground. Thank you.

Senator Collins.

Senator COLLINS. Thank you. Let me first endorse the Chairman's comments on liability and encourage you to take another look at our bill.

I want to follow up on the issue of how you handle critical infrastructure. In the statement, it says that the White House proposal emphasizes transparency to help market forces ensure that critical infrastructure operators are accountable for cybersecurity, and it goes on to say there would be new requirements for reporting to the Securities and Exchange Commission, that there would be publication of a summary of the evaluation results, and I must say, these provisions surprise me, and the reason that they surprise me is the list of critical infrastructure is now classified. Now, granted, I am sure that many Americans and many of those who would do us harm could obviously figure out what a lot of the critical infrastructure sites and capabilities are, but the fact is, the list is classified. So are you planning to change the classification and make the list public?

Mr. REITINGER. Thank you, Ranking Member Collins. This would actually be a different list and one that is of somewhat lower sensitivity. The list that you are referring to references or includes classified or tiered systems and assets.

Senator COLLINS. Yes.

Mr. REITINGER. This would actually be a list of entities as opposed to specific assets. So instead of, for example, this generation facility, it would be this company that owns a number of different generation facilities, and I think that is of a lower level of sensitivity, and, in fact, is much more broadly known to the public.

Second, if one is going to bring public transparency disclosure levers to bear, one needs to have that information open. So in this case, we drew the conclusion that the list of entities, of critical infrastructure entities, would need to be public in order to move forward in this way.

Senator COLLINS. But you also go on to say that there would be a summary of the security plan and the evaluation of that plan would be publicly accessible. My concern is, we do not want to give those who would do us harm a roadmap to how to attack our crit-

ical infrastructure. If, in fact, you publicize, even at a broader level, what the critical infrastructure is and then require publication of a summary of the security plan, and this part is the most troubling part to me—the publication of the evaluation of that plan, are you not providing very valuable information to not only cyber criminals, but perhaps terrorist groups or nation-states that are constantly trying to probe our systems? I am really surprised that you want that to be public.

Mr. REITINGER. Yes, ma'am. I understand. If you will note the section, it specifically requires that only a high-level description of the plan and only a high-level description of results would be published, and specifically requires that in the regulations to be developed by the Secretary that information not be reported to such a detail that it would impair the security of that entity.

In point of fact, critical infrastructure entities are tested and probed all the time. That is simply the nature. I do not believe that on the level of reporting we would intend to require in going forward that we will increase the level of risk of those entities. In fact, if the publication of the results causes such entities to say, well, we need to do a much better job, then the regime is going to be having the effect we intend in that they will rapidly move to enhance their own security.

Senator COLLINS. But that is a name and shame approach, essentially, that you are hoping that there will be public criticism or press scrutiny that will essentially embarrass these entities into doing a better job. To me, if they are not doing a good job, then DHS goes in and applies sanctions or requires a better security plan. I do not think the answer is to make the weakness public. And the fact is that even if, in your scenario, it encourages that entity to do a better job, it is also telling very sophisticated computer hackers that this is an entity that they should focus on and that has some security lapses.

I really hope you will take another look at that. I understand what you are trying to do, but I think that you are also giving information to the enemy.

Mr. REITINGER. Just a couple of comments, ma'am, and I appreciate that. I understand your level of concern, which is appropriate. What I would say is, briefly, it is not just that the entity would receive shame, but that the market would actually take that into account, that if you are a more secure entity as opposed to a less secure entity, then business partners and not just government may want to do work with the more secure entity because it gives them a higher level of assurance. So it is not just the name and shame. It is actually to drive market effects.

The second thing is we would intend that any publication of results be at such a high level that it would not increase the level of security, or the level of threat that an entity would face, but instead would merely make the public aware of the overall level of security.

Senator COLLINS. But if it is sufficient to cause a business to no longer do business with that entity, it is sufficient to wave a red flag at those who would do us harm. That is my point. I do not think you can have it both ways. If the vulnerability that is revealed or the poor evaluation that is published is sufficient to cause

other commercial entities to refrain from doing business with this section of the critical infrastructure, then surely it is going to be sufficient to prompt a computer hacker or terrorist group or Russia or China to redouble its efforts. I just think we need to think about that issue.

Let me just quickly switch to another issue, since my time is expiring rapidly. Mr. Schwartz, because of your background on privacy, and you have always been such a help to our Committee as we have wrestled with those issues, I want to talk to you about the idea of the national law for data breach reporting. My first reaction is that that is a good idea, that there should be more uniformity. I think it would be easier for consumers as well as for businesses to not have to figure out what an individual law in one of those 47 states that has them means in their particular case.

Are you talking about just a uniform nationwide reporting of breaches, or are you also talking about having uniform remedies for what a company has to do when there is a breach? I ask this not looking for any particular answer, but just to better understand what you are proposing.

Mr. SCHWARTZ. The focus is really on the reporting and making sure that consumers get the same information as the law enforcement and others that work on these issues receieve. Also, the focus is to make sure that they are getting the right information about the cases so that we can go after the bad guys when a breach has happened and is tied to something more than simply a lost laptop or something like that.

But, we need to try to figure out how to best get to that kind of level where consumers get the same information, and it is actionable. We think that what we have come up with moves us forward in that regard. We have had a lot of experimentation in the States. We have learned a lot from that. We think that it has been a useful avenue and that those laws have been successful. It is time to move forward and make sure that we can capitalize on that at this point.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Carper.

Senator CARPER. Just to follow up on the last question that Senator Collins was pursuing, and Mr. Chipman, feel free to jump in on this, as well. Former Senator Robert Bennett of Utah and I had worked on disclosure legislation in at least the last Congress, maybe the last two Congresses. We were on the Banking Committee, and this was an area where other committees had jurisdiction.

Do either of you know in the Administration's proposal what legislation you drew from in order to prepare and present the Administration's proposal in this regard?

Mr. CHIPMAN. I am not sure if we drew from that particular proposal. I think a number of different bills and ideas in this area were looked at.

Senator CARPER. We could never move the legislation forward because we were on the Banking Committee. We had some jurisdiction. The Commerce Committee had some jurisdiction. The Judiciary Committee, had some jurisdiction. Because of jurisdictional

grounds, we could never move anything forward. How have you acted this way to help us thread the needle here?

Mr. SCHWARTZ. Well, I think, again, coming back to this partnership between the different agencies involved, we had all of our equities lined up and tried to work together to develop this in a way that worked for all of the different jurisdictions that you would have to have issues with, where we could have this kind of conversation to move past some of those concerns.

Senator CARPER. I want to go back to another point that Senator Collins was making and talking a little bit about the name and shame. We got into a little discussion of how do we harness market forces to help drive good public policy behavior. We can have all the laws on the books, we can have regulations on the books, and we can have prosecutors out there trying to capture the bad guys and put them in jail, but to the extent that we can harness market forces to help us solve this problem or address these challenges, that is a very good thing. Does anybody want to talk a little bit more about that for us, please? Anybody at all?

Mr. SCHWARTZ. This comes back to how to get those incentives right, and we agree with the way that you framed it that market forces are extremely important, especially because we cannot expect the government to be able to go into all of these different areas that we are going to consider to be covered critical infrastructure in this space and have exact knowledge of how to operate in each of those areas from the beginning.

What we can do is to work in a public-private partnership, especially on the Internet, where we have so many public-private partnerships, and try and come up with solutions that work for the market. We feel as though the security plans process moves us much further down that line and that will help us build innovation in the mitigation strategies in a way that the government approach, the government coming in, cannot do.

Senator CARPER. All right. Thanks.

Mr. Chipman, the Administration's testimony mentioned that our critical cyber infrastructure is attacked repeatedly. We all know that. In addition, sensitive, personal, government, and business information is stolen online all the time. How often are we able to actually catch and successfully prosecute the individuals or the groups who commit these crimes? How will the Administration's proposal help further with these efforts?

Mr. CHIPMAN. Thank you. You are quite right. The amount of cyber crime, the number of intrusions, is growing, and they are challenging cases to bring, for sure. There is a level of anonymity on the Internet at times that make these hard cases to bring. Many times, there are actors outside of the United States and it is simply hard to find out where they are or who they are to bring cases against them, though we have had a fair amount of success in recent years. In 2009, I believe, there were over 150 cases brought. We have had a number of recent successes bringing down large organized crime rings engaged in mainly banking fraud and other types of computer intrusions to steal money, credit card numbers, and things like that.

I think the proposals in the Administration's cyber package will help in a number of ways. They will help harmonize laws relative

to penalties and will add a few tools to the tool box, for example, making clear that computer crimes are a RICO predicate. I think that will help and it will add to the tools that we can bring to bear in these cases.

Senator CARPER. All right. I am going to be leaving. I do not know if you all are going to stay on for another round here or not, but let me just ask you as we conclude here, or at least as my participation concludes, would you all just take maybe a minute apiece and reflect on what has been said here, what you have said, what you have heard others say, the questions that have been asked, and the answers given, and maybe just give us some concluding thoughts, starting with you, Mr. Chipman, then concluding with Mr. Reitinger.

Mr. CHIPMAN. Sure. Thank you very much. I think I am struck here by how collaborative, as Mr. Reitinger and others have mentioned, this process has been within the Executive Branch in terms of trying to, as Mr. Schwartz said, trying to get the balance right.

Senator CARPER. It reflects this Committee, does it not?

Mr. CHIPMAN. That is what I was about to say. And I am struck by what I hope is the start here of a very collaborative process with all of you and others, and I think I can fairly speak for the Administration in that regard.

Senator CARPER. All right. A closing thought, Mr. Schwartz? And I understand your father is here, is that right?

Mr. SCHWARTZ. That is right.

Senator CARPER. If we were to line all the men up here in this room in a row, do you think we could pick him out?

Mr. SCHWARTZ. He looks a lot like me. He is in town for a conference, and this just happened to work out.

Senator CARPER. There is no denying who your father is. We welcome your dad and thank him and your mom for instilling some really good values in you to get you to this place today.

Mr. SCHWARTZ. Thank you, Senator. So, briefly, the one thing I would say, it is on this point that you raised before about public-private partnerships and getting the market moving in the right area. Our work over the past year from the Internet Policy Task Force that Secretary Locke helped put together at the Commerce Department, we received a lot of comments from the private sector on this and I think they really are incentivized right now to try and move forward in the right way, at least those that have been paying attention to this space, and they want to move forward in the right way. I think we can put together those best practices that can build a framework for success in these different areas, and we should use that to our advantage now while we have it.

Senator CARPER. All right. Thank you.

Any closing thoughts, Mr. Butler?

Mr. BUTLER. Sure, Senator Carper. My sense is that it is collaboration and not being complacent with where we are, to continue to build on the collaboration. People have mentioned partnerships. It is interagency. It is with the Congress. It is certainly with industry and focusing on not just the easy areas, but the hard areas that we need to work through. As the Administration announced last week, there is an international aspect that needs to be taken into account as we move forward in time.

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

Mr. REITINGER. Thank you, Senator. Just briefly, I think it is important to recognize that we do not have all the answers in government. I do not think the private sector has all the answers and I do not think all the answers exist on the Hill. This is going to take all of us working together. This is not a question of, for example, the government coming in and saying, the private sector is not doing its job, it needs to do a better job, and it is pounding the table, or them coming in and saying the same thing. We need to find the right way to bring the capabilities of government together with the capabilities of the private sector, and we very much look forward to continuing to work with the Members of this Committee and Congress generally to make sure we get the balance right as cybersecurity legislation moves forward.

Senator CARPER. All right. Thanks. And as you prepare to weigh anchor and head out into the other uncharted waters, an old saying we have from my days in the Navy, is fair winds and a following sea. We thank you for your service and wish you Godspeed.

Mr. REITINGER. Thank you.

Chairman LIEBERMAN. Thanks, Senator Carper.

Thanks to all of our witnesses. Since I now know your father is here, Mr. Schwartz, I want to say in his presence, Senator Collins and I were remarking that by your testimony over the years, you have really built up a lot of credibility with the Committee. You have been straight ahead and presented your arguments well, never contentiously. Occasionally, we have a contentious witness from an advocacy group here. It is a pleasure to be able to share that private conversation in the presence of your father.

I thank all of you for the testimony. I want to come back and say that Senator Reid, I believe working with Senator McConnell, is now talking about setting up different groups to negotiate with the Administration on different parts of the bill to try to expedite it forward.

Senator Collins, I am under the impression that one of the things holding up the immediate initiation of those negotiations is something that is another favorite of yours and mine, and talk about irony, these folks are going to be testifying before five more committees of Congress, in the next week and a half, and therefore, their staffs are preoccupied with that and not able to initiate the negotiations.

We have had a longstanding interest pursuant to a recommendation of the 9/11 Commission to try to reduce the number of committees that people have to testify before. We have been pretty good at reforming the Executive Branch of Government, less successful at reforming the Legislative Branch.

Anyway, I thank you very much. We are really going to push full steam ahead here, to continue the nautical metaphors of Senator Carper, and hope to get this to the floor as soon as we possibly can, hopefully with a good consensus approach. But thank you for everything you have done, the considerable work that was done. We were impatient, but when you produced the Administration proposal, it was not an outline, it was legislation. It was quite comprehensive. And, of course, we like it because it is very much like

what we proposed in our Committee bill. So we look forward to taking it from here together to enactment.

We are going to keep the record of the hearing open for 15 days for any additional questions or answers. I thank Senator Collins, Senator Carper, and all of you.

And with that, the hearing is adjourned.

[Whereupon, at 12:23 p.m., the Committee was adjourned.]

APPENDIX

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

Opening Statement of Chairman Joseph Lieberman
"Protecting Cyberspace: Assessing the White House Proposal"
Homeland Security and Governmental Affairs Committee
May 23, 2011

Good morning. Thanks to everyone for being here, particularly the witnesses. If there is anyone who doesn't believe we urgently need to pass strong cybersecurity legislation, the topic of our hearing today, I would just ask them to look at some of the high-profile computer attacks that have happened in the past several months.

Let's take the Sony Corp. as an example. In two separate attacks, hackers stole the personal and billing information – including reportedly some of the credit card numbers – of 100 million people.

And when the site finally reopened last Thursday, the company found that it hadn't actually closed all the vulnerabilities that had been opened up in the wake of the first two attacks, and that hackers could still use the information to hijack people's accounts.

If that doesn't convince people we've got a real cybersecurity problem in America, consider the breaches that have occurred in the cyber systems of organizations that specialize in cybersecurity.

Take Oak Ridge National Laboratory, which has a very important role in the Department of Energy's mission to secure our electric grid from cyber attack, whether by enemy nations or cyber-terrorists. Oak Ridge was, itself, successfully cyber attacked just last month.

Or take a case that's been widely reported in the media: RSA, whose SecureID is used by some 40 million users in 30,000 companies - and parts of the federal government, including the Social Security Administration, the Department of Defense, and the United States Senate – had valuable security information stolen from its computers that could compromise these systems and actually be used in future attacks.

Bottom line, if we don't do something soon, the Internet is going to become a digital Dodge City. The internet is just too important to modern life to allow that to happen. This is a place that really calls out for law. It's time to say, if I may continue the Dodge City metaphor: "There's a new sheriff in town and we're going to have some law and order around here." We can do that without compromising, and in fact elevating, liberty and privacy.

The recent release of the White House's proposed Cybersecurity legislation is a very important step. I think it represents a turning point in our efforts to pass the strong measures we need to protect consumers, businesses, critical infrastructure and our national security from cyber attacks by terrorists, spies, or crooks.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

I am pleased not just by the presence of the Administration's cybersecurity legislation, but by its substance. The President's proposal is similar in many ways to legislation this Committee has been working on in the past two Congresses. And where there are differences, I think we can work together to find agreement. In this regard, I'm very grateful to the witnesses for appearing before us today. This is the first time the Administration has testified on its cybersecurity proposal since it was released.

One important area of agreement is the recognition that the Department of Homeland Security must be given the job of protecting the dot gov and dot com domains. In other words, DHS will be the new sheriff in cyber town that we need.

A crucial part of this job will be for DHS to identify critical cyber infrastructure – the systems or assets that control things like power plants, electric grids and pipelines, which if commandeered by our enemies could lead to havoc, death, and destruction. DHS needs that authority and also the ability to evaluate the risks to those systems.

Once those systems and risks have been identified, the owners and operators of these systems should be required to develop plans to safeguard their systems. Those plans would need to be reviewed to ensure they will actually improve security – reviewed by DHS in our legislation, by government-accredited, third party evaluators in the White House proposal.

Just last week we saw an example of both why this kind of planning is so necessary and why DHS has raised itself to a quality where it deserves to have the job. A private researcher had discovered a major security flaw in a widely-used industrial control system and was going to present his research at a conference.

When personnel at DHS discovered this and explained to the researcher how dangerous it would be to have this information out in public before the security flaws had been patched, the researcher voluntarily canceled his talk.

As another cybersecurity expert said of this vulnerability: "This is different from simply stealing money out of someone's bank account. Things could explode."

Besides securing critical infrastructure, our bill and the White House bill would direct DHS to work cooperatively and on a voluntary basis with the private sector and state and local governments to share cybersecurity risk and best practice information. The White House proposal also clears the way for industry to share cybersecurity information without having to worry about running afoul of various privacy statutes that impede information sharing now.

The business and government communities would be free to use this advice as best suits their needs. There would be no "one-size-fits-all" mandates or dictates.

Both the White House bill and our committee bill also contain robust privacy oversight to ensure that our broader cybersecurity efforts do not impact individual privacy or civil liberties.

And, finally, both of our proposals would also reform and update the Federal Information Security Management Act to require continuous monitoring and protection of our federal computer networks and do away with the current paper-based reporting system.

One key difference between our bill and the White House proposal is that our legislation creates a White House Office of Cybersecurity with a Senate-confirmed leader. We just believe that the stakes are too high, when it comes to cybersecurity for our country, that whoever holds this position should be confirmed by the Senate and therefore be accountable to Congress.

Our bill would also clarify the President's authority to act in the event of a true cyber emergency, while at the same time ensuring that the President cannot take any action that would limit free speech or "shut down" the internet. In its original version this section was misconstrued, and we have tried to reassure everybody about the very, very limited circumstances under which the President could act, and the limited range of his actions. The Administration believes that additional statutory authority is unnecessary because the President has the authority that we gave him in this proposal already in existing law.

Bottom line, the internet is a thrilling new frontier with a plugged-in population nearly 2 billion users – and growing everyday – that has created a revolution in commerce, communications, entertainment, finance and government - really, just about every aspect of our lives.

But it need not—must not--be a lawless frontier, and I believe that with the proposals we have in front of us, we can bring about the needed change this year to make the internet safer and more secure.

The majority leader, Senator Reid, has taken a very active interest in this legislation. It remains a priority of his for this session. I've said to him that I believe it's the most important piece of legislation coming out of our committee in this session. He is working with the Republican leader, Senator McConnell, and there are six different committees that claim some sort of jurisdiction over this subject matter. I believe it's the intention of Senate leadership to establish a process by which all those committees can, as quickly as possible, negotiate any remaining differences in the bills that have come out of committee so we can bring it to the Senate floor as quickly as possible.

We have had a very successful round of negotiations with the Commerce Committee, which is the other committee claiming major jurisdiction here, and we've resolved just about all of the differences that we had between us.

Now, before I turn this over to Sen. Collins, I wanted to take a moment to thank Phil Reitinger, who as Deputy Under Secretary for the National Protection and Programs Directorate, has done a great job in a relatively short period of time and really been a leader in the Administration in crafting this White House proposal, including working very productively and cooperatively with our Committee.

With the bill finalized, Phil has decided to move on to the next great chapter of his life. Phil, I want to wish you the best of luck and thank you for your public service, which has made a real difference to our country.

Sen. Collins.

-30-

Statement of
Senator Susan M. Collins

"Protecting Cyberspace: Assessing the White House Proposal"

May 23, 2011

★ ★ ★

I am pleased that the Administration is now fully engaged on the imperative issue of cyber security.

Experts believe that the cyber arena is where the biggest gap exists between the threat level and our preparedness.

Virtually every week we learn of another massive cyber breach. The company that authenticates users seeking to access Senate networks was hacked. Sony's on-line gaming network was breached. We read in this morning's newspaper that the repressive government of Syria attacked the social media sites of protestors. The number and sophistication of cyber attacks continue to grow every day.

The FBI reports that small and medium-size businesses in the U.S. lost more than $11 million over the past year in on-line scams in which stolen banking credentials were used for fraudulent wire transfers to companies in China. Worldwide, the annual cost of cyber crime has climbed to more than $1 trillion. And according to testimony last year from the Senate Sergeant at Arms, on average, each month 1.8 billion cyber attacks target the computer systems of Congress and Executive Branch agencies.

Unfortunately, the government's overall approach to cyber security has been disjointed and uncoordinated. The threat is too great to allow this to continue. The need for Congress to pass comprehensive cyber security legislation is more urgent than ever.

So I am pleased that the White House has now joined the efforts this Committee has undertaken over the past few years to develop legislation to help safeguard the American people from a cyber 9/11.

I am also encouraged that the Administration's approach is similar, in many respects, to our framework.

Both bills call for a strong public/private partnership to improve cyber security. Our bill would bolster sharing, within the private sector and with government, of actionable threat intelligence that would help

protect the private sector from advanced cyber threats. It would also direct the Department of Homeland Security to collaborate with the private sector to develop and promote cyber security best practices.

Like our bill, the White House proposal recognizes the Department of Homeland Security as the appropriate agency to lead the federal effort to secure federal civilian agencies, the ".gov" domain, as well as infrastructure against cyber threats. I believe that cyber security at DHS must be led by a strong and empowered director who can close the coordination gaps that currently exist. This leader should report directly to the Secretary of Homeland Security and also serve as a principal advisor to the President on cyber security.

The Administration's approach to securing the nation's most critical infrastructure is similar to the risk-based approach in our bill.

Our bill differs, however, in providing liability protection as an incentive for companies to maintain continuous compliance with risk-based performance requirements.

We should also detail the extent of the President's authority to deal with cyber emergencies. Our current bill has explicit provisions preventing the President from shutting down the Internet. It also places limits on the length of any emergency actions, requires reporting to Congress, ensures remedial actions are the least disruptive steps feasible, and includes privacy protections.

By contrast, the Administration appears to rely on outmoded, yet potentially sweeping, authorities granted in the Communications Act of 1934.

Our bill explicitly calls for the development of a supply chain strategy to leverage the federal government's buying power to drive improvements in cyber security, which should have beneficial ripple effects in the larger commercial market. As a large customer, the federal government can contract with companies to innovate and improve the security of their IT services and products. These innovations could lead to new security baselines for services and products offered to the private sector and the general public without mandating specific market outcomes.

In addition, our bill would give DHS much needed ability to hire and retain highly qualified cyber security professionals.

I look forward to hearing from our witnesses today and to the passage of comprehensive cyber legislation.

Statement for the Record
Of

Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Robert J. Butler
Deputy Assistant Secretary of Defense for Cyber Policy
Department of Defense

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology
Department of Commerce

Jason Chipman
Senior Counsel to the Deputy Attorney General
Department of Justice

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

May 23, 2011

Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is an honor for us to appear before you today to discuss the critical issue of cybersecurity. Specifically we plan to address the Administration's legislative proposal to improve cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

The Nation's digital infrastructure is fundamental to our economy, critical to our national security and defense, and essential for open and transparent government. Today, however, the same technologies that empower our citizens and organizations for good can be misused by some for harm.

The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and limited comprehensive threat and

vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade.

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

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

Recognizing the serious nature of this challenge, the President made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The President also highlighted the importance of sharing responsibility for cybersecurity, working with industry to find solutions that improve security and promote prosperity.

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Through this ongoing work, it has become clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated. We will never be fully insulated from cyber attacks. However, these proposals provide important steps in improving the cybersecurity posture of the United States. Members of both parties in Congress have come to the same conclusion as approximately 50 cyber-related bills were introduced in the last session of Congress. Senate Majority Leader Reid and six Senate committee chairs thus wrote to the President and asked for his input on cybersecurity legislation, while Members from both sides of the aisle have remained steadfast in their resolve to act. The Administration welcomed the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider as it moves forward on cybersecurity legislation. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace.

The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

Protecting the American People

1) National Data Breach Reporting. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements with a clear and unified nationwide requirement. It also helps ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

2) Penalties for Computer Criminals. The laws regarding penalties for computer crime are not fully synchronized with those for other types of crime. For example, a key tool for fighting organized crime is the Racketeering Influenced and Corrupt Organizations Act (RICO). Yet RICO does not apply to computer crimes, despite the fact that they have become a big business for organized crime. The Administration proposal thus clarifies the penalties for computer crimes, synchronizes them with other crimes, and sets a mandatory minimum penalty for attacks that damage or shut down computers that control our critical infrastructure.

Protecting our Nation's Critical Infrastructure

Our safety and way of life depend upon our critical infrastructure as well as the strength of our economy. The Administration is already working to protect critical infrastructure from cyber threats, but we believe that the following legislative changes are necessary to better protect this infrastructure:

1) Voluntary Government Assistance to Industry, States, and Local Government. Organizations that suffer a cyber intrusion often ask the Federal Government for assistance with fixing the damage and for advice on building better defenses. For example, organizations sometimes ask DHS to help review their computer logs to see when a hacker broke in. However the lack of a clear statutory framework describing DHS's authorities has sometimes slowed the ability of DHS to help the requesting organization. The Administration proposal will enable DHS to quickly help a private-sector company, state, or local government when that organization asks for help. It also clarifies the type of assistance that DHS can provide to the requesting organization.

2) Voluntary Information Sharing with Industry, States, and Local Government. Businesses, states, and local governments sometimes identify new types of computer viruses or other cyber threats or incidents, but they are uncertain about whether they can share this information with the Federal Government. The Administration proposal makes clear that these entities can share information about cyber threats or incidents with DHS. To fully address these entities' concerns, it provides them with immunity when sharing cybersecurity information with DHS. At the same time, the proposal mandates robust privacy oversight to

ensure that the voluntarily shared information does not impinge on individual privacy and civil liberties.

3) Critical Infrastructure Cybersecurity Risk Mitigation. The Nation's critical infrastructure, such as the electricity grid and financial sector, is vital to supporting the basics of life in America. Market forces are pushing infrastructure operators to put their infrastructure online, which enables them to remotely manage the infrastructure and increases their efficiency. However, when our infrastructure is online, it is also vulnerable to malicious cyber activities that could cripple essential services. Our proposal emphasizes transparency to help market forces ensure that critical-infrastructure operators are accountable for their cybersecurity.

   The Administration proposal requires DHS, in consultation with the appropriate agencies, to work with industry to identify the Nation's core critical infrastructure and to prioritize the most important cyber risks to that infrastructure. Representatives of critical infrastructure entities and standards setting organizations would then work together to propose standardized risk mitigation frameworks which focus not on compliance but instead on increasing actual security in a cost-effective manner. Then, each critical-infrastructure operator would propose a plan that identifies the steps it will take to address the identified risks as guided by the applicable framework. Each critical infrastructure entity's plan will be assessed by a third-party, commercial evaluator. Companies that are already required to report to the Security and Exchange Commission (SEC) would also have to certify to the SEC that they had developed and were implementing a risk mitigation plan. A high-level summary of the plan and the evaluation results would be publically accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify or produce a new framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial evaluators.

Protecting Federal Government Computers and Networks

Over the past five years, the Federal Government has greatly increased the effort and resources we devote to securing our computer systems. While we have made major improvements,[1] updated legislation is necessary to reach the Administration goals for Federal cybersecurity, so the Administration's legislative proposal includes:

1) Management. The Administration proposal would update the Federal Information Security Management Act (FISMA) and formalize DHS' current role in managing cybersecurity for the Federal Government's civilian computers and networks, in order to provide departments and agencies with a shared source of expertise. The legislation would also promote the ongoing transformation of FISMA toward increased automation and performance based security measures.

[1] *See* GAO, *.Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, March 5 2010.

2) Personnel. The recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, so we need to be sure that the government can recruit and retain these talented individuals. Our legislative proposal will give DHS more flexibility in hiring these individuals. It will also permit the government and private industry to temporarily exchange experts from the other, so that both can learn from each others' expertise.

3) National Cybersecurity Protection Program. The Administration proposal directs DHS to establish a program to actively protect federal systems and to continue the DHS efforts that are underway in this area. This program will include activities such as deploying intrusion detection and prevention capabilities, conducting risk assessments, and providing incident response and other technical assistance. DHS conducts many of these activities today under existing authority. For example, DHS is deploying what is referred to as the National Cybersecurity Protection System – of which the EINSTEIN intrusion detection and prevention capabilities are a key component. The EINSTEIN system helps block malicious actors from accessing federal executive branch civilian agencies, while DHS works closely with those agencies to bolster their own defensive capabilities. Despite progress in this area, deploying EINSTEIN to new agencies has sometimes been slowed due to the need for lengthy reviews and interagency agreements. To address this issue, the proposal will clarify DHS' authorities to protect federal systems. At the same time, strong privacy and civil liberties protections have been incorporated into the provision to protect the rights of federal employees and other users of federal systems.

4) Data Centers. The Federal Government has embraced cloud computing, where computer services and applications are run remotely over the Internet. Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law.

Protecting Individuals' Privacy and Civil Liberties

The Administration's proposal ensures the protection of individuals' privacy and civil liberties through a framework designed expressly to address the challenges of cybersecurity.

- It requires DHS to implement its cybersecurity program in accordance with privacy and civil liberties procedures. These must be developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All federal agencies who would obtain information under this proposal will follow privacy and civil liberties procedures, developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All monitoring, collection, use, retention, and sharing of information is limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement purposes only with the approval of the Attorney General.

- When a private-sector business, state, or local government wants to obtain immunity in connection with sharing of information with DHS, it must first make reasonable efforts to remove identifying information unrelated to cybersecurity threats.
- The proposal also mandates the development of layered oversight programs and congressional reporting.
- Immunity for the private sector business, state, or local government is conditioned on its compliance with the requirements of the proposal.

Taken together, these requirements create a new framework of privacy and civil liberties protection designed expressly to address the challenges of cybersecurity.

Conclusion

Our Nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress as they move forward on this issue.

Post-Hearing Questions for the Record
Submitted to Philip R. Reitinger, Robert J. Butler, Ari Schwartz, Jason C. Chipman
From Senator Daniel K. Akaka

"Protecting Cyberspace: Assessing the White House Proposal"
May 23, 2011

Question#:	1
Topic:	workforce
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: I was very concerned with some of the workforce provisions in the cybersecurity bill the Committee considered last year. Aligning the new Department of Homeland Security (DHS) hiring and pay authorities to current Department of Defense authorities addresses my concern with creating new workforce authorities for a specific workforce group that are not consistent with any other workforce's authorities, but I still have concerns that the hiring and pay flexibilities may be too broad or may put other agencies at a competitive disadvantage.

Please describe the workforce recruiting and retention challenges at DHS that you believe justify these authorities.

The Office of Personnel Management granted DHS direct hiring authority for 1000 excepted service cybersecurity positions in 2009. How many employees has DHS hired under this authority?

The legislation would remove the numerical limitation on DHS's current direct hire authority. What additional hiring flexibility, if any, does DHS believe the requested authority would provide? Why is the direct hire request made without time or numerical limit?

Response: Attracting and retaining highly qualified technical cybersecurity experts to join government service over the high-paying private sector can be difficult, especially when the private sector can often hire an individual much more quickly than the government. Moreover, hiring and pay authorities vary within the Federal government as well, making it challenging for some agencies to recruit cyber talent. While the Department of Homeland Security (DHS) and the Department of Defense (DoD) have parallel cybersecurity responsibilities for protecting civilian government and military networks, respectively, the DoD currently has greater flexibility to recruit and retain cybersecurity experts. In recognition of DHS's increased cybersecurity responsibilities,

Question#:	1
Topic:	workforce
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

the proposal provides the Secretary of Homeland Security with hiring and pay authorities commensurate with those of DoD.

Specifically, the Administration proposes authorizing the Secretary to establish positions in the excepted service, such that the Secretary could make direct appointments (10 U.S.C. §1601), set compensation rates (10 U.S.C. §1602), and pay additional benefits and incentives (10 U.S.C. §1603). The Secretary would also be authorized to establish a scholarship program for employees to pursue an associate, baccalaureate, advanced degree, or a certification in an information assurance discipline (10 U.S.C. §2200a). These authorities would be limited to only those employees performing functions related to the security of federal systems or critical information infrastructure.

A temporary Schedule A authority was granted by the Office of Personnel Management (OPM) to DHS in September 2009 for those certain cybersecurity occupations. As of July 2011, 217 positions have been filled using the Schedule A authority.

This authority is set to expire on December 31, 2012 and also does not cover many of the cybersecurity occupations at DHS.

The proposed legislation granting DHS the same personnel authorities as DoD with respect to cybersecurity positions would greatly help to fill this gap and address cyber recruitment and development issues for DHS. Consistent with the DoD workforce authorities, the proposed legislation would not impose limitations on the number of covered employees or the time period of the alternative authorities. We expect the demand for skilled cyber professionals to increase for the foreseeable future, and imposing such limitations would severely hinder DHS's ability to recruit a workforce to effectively address cybersecurity challenges.

Question: The proposal grants DHS the hiring and pay authorities that the Department of Defense has under sections 1601, 1602, and 1603(a) of title 10. The proposal, however, would omit the pay authority in section 1603(b), which grants Cost of Living Allowances (COLA) to Defense intelligence employees stationed outside the continental United States or in Alaska when justified by the cost of living or environmental conditions. Why was section 1603(b) omitted, and does the Department intend to pay COLA pursuant to 1603(b) or 5 U.S.C. § 5941 to any employees stationed in the applicable areas?

Response: The Non-Foreign Area Retirement Equity Assurance Act (the Act) as contained in subtitle B (sections 1911-1919) of title XIX of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 (Public Law 111-84, October 28, 2009) transitions the non-foreign area cost-of-living allowance (COLA) authorized under 5

Question#:	1
Topic:	workforce
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

U.S.C. 5941(a)(1) to locality pay authorized under 5 U.S.C. 5304 in the non-foreign areas as listed in 5 CFR 591.205. The Act also extends locality pay to American Samoa and other non-foreign territories and possessions of the United States where no COLA rate applies. The locality pay will be phased in over a three-year period beginning in January 2010 and ending in January 2012, when the full applicable locality rate will be used. As locality pay increases, payable COLA rates must be reduced. As a consequence, in the remaining years employees may receive both locality pay and reduced COLA rates for a number of years and no new COLA rates will be established for the non-foreign areas. However, to ensure that DHS employees continue to receive tax-free residual COLA under section 5941 during the remaining years, DHS agrees the legislative proposal may need to be clarified.

Question: What analysis, if any, has the Administration conducted regarding the recruitment and retention effects these authorities would have on other agencies that employ cybersecurity professionals, and what are the results of any such analysis?

Response: DHS has not conducted an analysis on the recruitment and retention effects these personnel authorities will have on other agencies.

DHS plays a unique, leadership role in Federal cybersecurity efforts. By law and policy, DHS has multiple roles in U.S. cybersecurity, including protecting the federal executive branch civilian agencies (the "dot-gov"), coordinating the protection of critical infrastructure, investigating cyber related crimes, and supporting USCYBERCOM through the U.S. Coast Guard. In that capacity, DHS provides services to other Federal agencies to assist with their cybersecurity efforts. DHS also works with the Federal agencies that have primary responsibility for each critical infrastructure sector of the economy to ensure that the private sector has access to the technical resources it needs to protect itself. As DHS builds its cyber workforce, all agencies benefit. It is because of this unique role that it is of utmost importance that DHS recruit and retain the most highly qualified cybersecurity specialists.

Question#:	2
Topic:	protections
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: This bill provides that DHS shall apply civil service protections under 2301 or title 5, as well as "1612(b) of title 10 with respect to the exercise of authority under section 1601 of title 10." With the exception of employees serving in positions converted to excepted service under section 1601 without a break in service, section 1612(b) would not provide anti-discrimination, whistleblower, anti-nepotism, and other protections from prohibited personnel practices under section 2302 of title 5, nor the right to appeal adverse actions to the Merit Systems Protection Board (MSPB) under chapter 75 of title 5, to employees serving in positions established under the authority granted in this legislation.

Does the Administration intend to exclude DHS employees hired under the authority granted in this legislation from the protections included in section 2302 and chapter 75 of title 5?

Response: No, DHS does not intend to exclude DHS employees hired under this new authority from the protections in Section 2302 and chapter 75. Employees covered by merit system principles under Section 2301 of title 5 are inherently covered by the prohibited personnel practices under section 2302. However, we would be happy to work with Congress as the legislation progresses to ensure that these protections apply.

Question: If so, what is the scope of this exclusion – is it limited to hiring and pay decisions made with "the exercise of authority under section 1601" or would these employees be excluded from sections 2302 and chapter 75 of title 5 for all purposes?

If exclusion from the protection of section 2302 and chapter 75 is intended, please provide the justification for that exclusion.

The merit system principles under section 2301 of title 5 would apply to these employees. If exclusion from the protection of section 2302 and chapter 75 is intended, please explain how these merit system principles would be enforced.

Response: DHS employees hired under the authority granted in this legislation would not be excluded from the protections included in section 2302 and chapter 75 of title 5. We agree the legislative proposal may need to be clarified to ensure civil service protections are applied under section 2302 and chapter 75.

Question#:	2
Topic:	protections
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The Administration has supported legislative efforts to extend whistleblower protections to employees of the Transportation Security Administration and Intelligence Community employees. Would the administration propose that employees hired under this legislation be granted whistleblower protections under title 5, under the proposed new Intelligence protections, or neither?

Response: The Administration would support efforts to extend whistleblower protections to DHS employees hired under the authority granted in this legislation.

Question#:	3
Topic:	Section 248
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: According to Section 248 of the Administration's cybersecurity legislative proposal, the Privacy and Civil Liberties Oversight Board is tasked with assessing the privacy and civil liberties impact of the government's activities under the new cybersecurity law and suggesting any needed changes. However, to date, the Board has not been stood up.

Please elaborate on the role the Administration envisions for the Board to ensure that this legislation does not negatively affect privacy and civil liberties.

Response: The Federal government's cybersecurity responsibilities are distributed across multiple departments and agencies, each with a different mission. The Privacy and Civil Liberties Oversight Board (PCLOB) will be uniquely positioned in an oversight role, independent of any particular department or agency, advising the Administration on the privacy, civil rights, and civil liberties impact of government-wide and interagency cybersecurity policies and activities.

Question: Will the Administration commit to prioritizing nominations for the Board to allow it to carry out its mission prior to the implementation of this legislation?

Response: The Administration remains committed to privacy and civil liberties protections. Two nominations for the Board have already been made, and the Administration will continue to work with Congress on this matter.

Question: If this legislation is implemented before the Board begins operating, how would the Administration ensure that privacy and civil liberties are vigorously protected under this proposal?

Response: The proposed legislation contains several additional requirements to ensure privacy and civil liberties protections are secured at all levels of government cybersecurity activities. The proposal will increase oversight, assessments, and congressional reporting from the privacy and civil liberties officials in DHS and the Department of Justice (DOJ). The proposal will also mandate consultation with outside privacy and civil liberties experts in the development of procedures, which themselves must be approved by the Attorney General. Simultaneously, each department and agency will maintain privacy, civil rights and civil liberties protections for its own programs. As a group, the department and agency Chief Privacy, Civil Rights and Civil Liberties Officers will continue to collaborate, share best practices, and ensure holistic protections

Question#:	3
Topic:	Section 248
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

across the government. A prime example of the existing close collaboration between departments and agencies on matters of privacy, civil rights and civil liberties is the coordinated effort between DHS and the Department of Defense (DoD), embodied in the National Protection and Programs Directorate's Office of the Director of Cybersecurity Coordination. In this office, DHS staff – including staff from the DHS Privacy Office, DHS Office for Civil Rights and Civil Liberties, and the DHS Office of General Counsel – are physically located inside the National Security Agency so they can work closely with their DoD counterparts. In addition, the Deputy Secretaries of DHS and DoD meet monthly to reinforce collaboration and coordination between the two departments on issues such as the protection of privacy and civil liberties.

Question#:	4
Topic:	Section Section 245(a)(1)
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The Administration's proposal to add new Subsection E to Title II of the Homeland Security Act provides avenues for the government to collect vast amounts of personal information. Section 245(a)(1) allows private sector entities to share any information with the Department of Homeland Security (DHS) for a cyber security purpose. It also requires "reasonable" efforts to remove identifying information that is unrelated to the cyber security threat.

Additionally, section 245(a)(2) allows federal agencies to share cyber security information with certain agency employees, DHS, and private entities providing certain computing and communication services, without corresponding restrictions on disclosure of identifying information. Similarly, section 245(b) allows DHS to disclose information to "appropriate governmental and private entities" without any requirement of removing identifying information.

Sections 245 and 246 waive all current legal constraints on information sharing and provide that disclosures authorized by this subtitle are not subject to any civil or criminal actions.

Why is the Administration seeking such a broad statutory waiver?

Answer: We believe that an effective information sharing provision is a vital component of a successful cybersecurity strategy. Without an ongoing exchange of information about rapidly evolving cyber threats and vulnerabilities, both the private sector and the Government will be ill-prepared to respond to and prevent destructive cybersecurity incidents. However, some Federal statutes restrict the collection and dissemination of information in a manner that is inconsistent with the type of largely automated monitoring conducted by contemporary, widely used cybersecurity systems such as intrusion detection and intrusion prevention systems. Moreover, the applicability of information sharing limitations found in some statutes are sufficiently unclear that they discourage information sharing that should be taking place between the private sector and the Government and among Government agencies. We believe that our proposal addresses these issues in a manner that balances the need to clarify the legality of appropriate information sharing and the requirement that privacy and civil liberties be protected

Question: What specific laws, if any, is the Administration seeking to override?

Question#:	4
Topic:	Section Section 245(a)(1)
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Answer: The number of statutes that restrict the disclosure of information in a manner that may affect cybersecurity programs—particularly network traffic monitoring for cybersecurity purposes—is both sizeable and difficult to catalog. It includes statutes commonly referred to as "electronic surveillance statutes" (e.g., the Wiretap Act, the Pen Register/Trap and Trace Statute, and the Stored Communications Act), but it also includes other statutes. For instance, while operating an intrusion detection system on behalf of Federal agencies, DHS personnel may incidentally view information from any of the agency networks it is protecting. The information that might be viewed in relation to such monitoring could include grand jury information, patient information, census data, and trade secret information; the disclosure of such information is subject to statutory restrictions. While there would be policies and procedures in place protecting such incidentally disclosed information and directing how DHS personnel must handle incidentally disclosed information, the permissibility of such information being exposed to DHS in the first place is unclear.

There are numerous statutes that prohibit the disclosure of information possessed by Federal agencies with a variety of disparate requirements; none of them contemplate the type of incidental disclosure associated with now commonplace network security technology such as an intrusion detection system. Creating independent exemptions for each of the statutes that might apply to all of the various types of information that the Government possesses would be impractical. Consequently, our proposal includes a clause that would permit the private sector to share information with the Government—and the Government to disseminate information internally and its service providers—for purposes of protecting their networks from cybersecurity threats, notwithstanding any other provision of law.

Question: What protections, if any, would be provided to the sharing or disclosure of identifying information that is related to a suspected cyber security threat?

Answer: We recognized that removing information sharing obstacles through the use of the "notwithstanding any other provision of law" clause could raise potential privacy and civil liberties concerns. Accordingly, we drafted section 245 with the numerous safeguards identified in our answer to question 1 to curb the possibility of abuse, whether intentional or accidental: with respect to identifying information in particular, our proposal requires that reasonable efforts be undertaken to remove information that can be used to identify specific persons unrelated to the cybersecurity threat before any disclosure is made under section 244 related to monitoring Federal systems or section 245(a)(1) related to private sector-to-Government information sharing and that policies and procedures required by section 248 safeguard such information.

Question#:	4
Topic:	Section Section 245(a)(1)
Hearing:	Protecting Cyberspace: Assessing the White House Proposal
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Why are federal agency disclosures under sections 245(a)(2) and 245(b) not subject to the same restriction on sharing identifying information that is incorporated in section 245(a)(1)?

Answer: Section 245(a)(1) authorizes private sector information sharing with the Government. Thus, the information that might be shared under that provision may contain personally identifiable information that the Government need not possess. In contrast, the information that could be disclosed under section 245(a)(2) and further disclosed under section 245(b) consists of information that is already in the Government's possession and, therefore, has already been subjected to existing laws and policies related to the retention and dissemination of personally identifiable information.