CYBERSECURITY: ASSESSING THE NATION'S ABILITY TO ADDRESS THE GROWING CYBER THREAT

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 7, 2011

Serial No. 112–73

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

71–615 PDF WASHINGTON : 2011

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana
JOHN L. MICA, Florida
TODD RUSSELL PLATTS, Pennsylvania
MICHAEL R. TURNER, Ohio
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
CONNIE MACK, Florida
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
ANN MARIE BUERKLE, New York
PAUL A. GOSAR, Arizona
RAÚL R. LABRADOR, Idaho
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
JOE WALSH, Illinois
TREY GOWDY, South Carolina
DENNIS A. ROSS, Florida
FRANK C. GUINTA, New Hampshire
BLAKE FARENTHOLD, Texas
MIKE KELLY, Pennsylvania

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
EDOLPHUS TOWNS, New York
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
DANNY K. DAVIS, Illinois
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
JOHN A. YARMUTH, Kentucky
CHRISTOPHER S. MURPHY, Connecticut
JACKIE SPEIER, California

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
ROBERT BORDEN, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

CYBERSECURITY: ASSESSING THE NATION'S ABILITY TO ADDRESS THE GROWING CYBER THREAT

THURSDAY, JULY 7, 2011

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 9:33 a.m. in room 2154, Rayburn House Office Building, Hon. Darrell E. Issa (chairman of the committee) presiding.

Present: Representatives Issa, Burton, Platts, Jordan, Chaffetz, Amash, Buerkle, Gosar, Labrador, Meehan, DesJarlais, Gowdy, Farenthold, Kelly, Cummings, Norton, Kucinich, Tierney, Connolly, Quigley, and Langevin.

Staff present: Ali Ahmad, deputy press secretary; Thomas A. Alexander, senior counsel; Michael R. Bebeau, assistant clerk; Robert Borden, general counsel; Lawrence J. Brady, staff director; Adam P. Fromm, director of Member services and committee operations; Linda Good, chief clerk; Christopher Hixon, deputy chief counsel, oversight; Mitchell S. Kominsky, counsel; Jim Lewis, senior policy advisor; Laura L. Rush, deputy chief clerk; Sang H. Yi, professional staff member; Jennifer Hoffman, minority press secretary; Carla Hultberg, minority chief clerk; Amy Miller, minority professional staff member; Dave Rapallo, minority senior counsel; and Carlos Uriarte, minority counsel.

Chairman ISSA. The committee will come to order.

The Oversight Committee exists to secure two fundamental principles: first, Americans have a right to know that the money Washington takes from them is well spent; and second, Americans deserve an efficient, effective government that works for them.

Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn responsibility is to hold government accountable to taxpayers because taxpayers have a right to know what they get from their government. We will work tirelessly in partnership with citizen watchdogs to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

Today's hearing is the first in what will likely be a long series of committee hearings related to the nature, extent and threat to America's digital infrastructure. On May 25th, the Subcommittee on National Security and Homeland Defense and Foreign Operations held a hearing on the issue that focused on the importance

of strategic public-private partnership to effectively combat the threat we face.

The important work that our colleague Mr. Chaffetz began will continue both at the subcommittee and the full committee. His groundwork and this committee's continued focus on what spans all of government, all of the private sector and, as we know every day, more of all of the world, is critical.

Today, we have representatives from each of the major areas of government that are often not seen together but are critical to implementing a plan which includes initiative by the President, a task force by the Republicans, a similar effort by Democrats and this committee, on a bipartisan basis, to ensure that both the House and the Senate act on the President's proposal in a timely fashion and recognize that the vulnerabilities, both public and private, which are well known, are, in fact, growing every day.

Our vulnerability is not just because of enemies well know, but can often be because of enemies unknown, enemies who simply have a grudge against society. It is today possible to be a great warrior with nothing but your slippers and your bedroom and the desire to bring down some aspect of public or private infrastructure related to the Internet.

A recent Office of Management and Budget report revealed that the number of cyber incidents affecting U.S. Federal agencies shot up 39 percent in 2010. The committee has even heard reports that potential U.S. losses of intellectual property last year could exceed $240 billion. Unfortunately, there is no reliable data and it is unlikely that this committee can see that that type of data is produced. It is clear we will continue to have losses. Some of those losses are unavoidable. If you leave your door open, you can lose the contents of your house.

Today, we are going hear about efforts to make sure that at least in the public sector, in cooperation with private enterprise, we are attempting to provide the locks and the master key system to ensure that you have the ability to close that door if you do all that can be done.

Cyber security is not simply for the large reports. Often the people hacked the most are small companies, companies who are not particularly targeted but ultimately might have great losses. One of the areas of concern in the President's proposal is in fact the vast reporting requirements. We want to ensure that information is a two-way street and that this not simply be about a way to empower the trial lawyers to ensure that someone who doesn't report in a timely fashion, particularly a smaller company that may be somewhat unaware as to the loss, doesn't find themselves simply being victimized by a lawsuit having been victimized by a hacker.

It is important to note that cyber threats are forever changing and that cyber attacks are always adapting to get around our defenses. This committee is ideally suited to evaluate the Federal Government's strategy and ability to counter these threats by both defensive and most importantly potentially, offensive innovations.

Recently, the Secretary of Defense, Robert Gates, stated that cyber attacks were an act of war. War is not a defensive only measure. War is something that, at times, needs to have a counterattack. Practically every committee of Congress can claim jurisdic-

tion over cybersecurity because of the uniquely expansive nature of the threat, the strength of our Nation's commerce, utilities, transportation, banking, telecommunications and national defense all depend on nimble response and aggressive cybersecurity infrastructure.

We claim no special jurisdiction here today, just the opposite. The Committee on Government Reform claims to be a conduit for all committees. We will be joined by one or more individuals from other committees and this committee will welcome other individuals to be allowed to sit on the dais and to participate in future hearings because we view our committee as a conduit for all committees, recognizing that any proposal, although it may well originate from this committee or pass through this committee, will also likely pass through virtually every committee of the Congress.

In closing, not since the end of World War II has America seen a threat so great looming for so long. As we led up to World War II, we had plenty of warning that the Fascists were a threat. We watched them arm, we saw them attack others, and we did little to prepare. Today, we have bolstered many defenses, but let us understand there is a difference between World War II and today.

We as a Nation, have already been attacked during my opening statement thousands of times. Attacks go on every day. Because one doesn't appear to be as large as Pearl Harbor doesn't change the fact that sooner or later, America will have to respond in a more aggressive fashion to some and be better prepared defensively for others.

With that, I would recognize the ranking member for his opening statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

I thank you very much for holding this hearing today.

In testimony before the House Intelligence Committee earlier this year, then CIA Director Leon Panetta called cybersecurity the battleground for the future. Our Nation's critical infrastructure, including power distribution, water supply, telecommunications and emergency services, has become increasingly dependent on computerized information systems to manage their operations and to process, maintain and report essential information.

Our government's national defense and critical information systems are also becoming increasingly reliant on information technology systems and Web-based transactions and services. Successful attacks on these systems threaten our troops, impair vital Federal programs and jeopardize the privacy of citizens whose personal information is maintained in government computer systems.

Mr. Chairman, I have served on the Naval Academy Board of Visitors of the last 10 years and we have recently made it a priority to change our curriculum so that every midshipman and woman is required now to take defensive courses with regard to cybersecurity.

In the last Congress, Members of the House and Senate introduced at least 50 cybersecurity related bills to address these issues. Given that urgency and the complexity of these challenges, congressional leadership called on the administration to help develop comprehensive cybersecurity legislation.

On May 12th, the Obama administration issued a legislative proposal that would significantly strengthen our ability to guard against cyber attacks. I applaud the President for his leadership on this issue and for creating a strong legislative framework to help Congress complete this important work.

For example, the administration's proposal would make key changes to the Federal Information Security Management Act including shifting to continuous monitoring and streamlined reporting for all Federal systems. I supported similar legislation last year and the committee successfully reported bipartisan legislation that would have achieved these goals. I am glad to see the administration's proposal has incorporated many of the improvements included in that legislation.

There are several provisions in the administration's proposal that I would like to see strengthened. First, I hope we will consider the creation of a Senate confirmable official with authority to set administration-wide cybersecurity policy. It is important that the official responsible for implementing FISMA have the authority to task all civilian departments and agencies with implementation of the Federal security standards.

The administration's proposal also creates a framework to ensure that the Federal Government and private industry are working together to protect our critical infrastructure. Private industry owns approximately 85 percent of the Nation's critical infrastructure and the administration's proposal allows critical infrastructure operators to develop their own frameworks for addressing cyber threats.

However, while there is room for healthy debate, even industry agrees that some level of government oversight is necessary to protect the American public from the potentially devastating consequences of a cyber attack.

At a recent hearing before the National Security Subcommittee, Tech America President, Phil Bond, testified that education and information sharing alone are inadequate to protect critical infrastructure and that the government rules, regulations and requirements are necessary to secure the Nation's critical infrastructure.

Other parts of the administration's proposal attempt to help consumers and companies by creating uniform reporting standards to address cyber attacks that result in breaches of personally identifiable consumer information. However, the proposal also would allow any entity to share with DHS personally identifiable information that otherwise could not be shared under existing law.

I agree that we should encourage information sharing between industry and government, but we also have to be careful that personally identifiable information is appropriately protected and shared with the government only when necessary.

Finally, I agree that law enforcement should have every tool necessary to go after hackers. I am concerned that the imposition of mandatory minimum sentencing unduly interferes with judges' discretion to set appropriate penalties. I hope that future drafts of the legislation will not include this specific provision.

I would like to thank Chairman Issa for agreeing to include our distinguished colleague, Congressman Jim Langevin, in our hearing today. Jim has been a leader on cybersecurity for many, many years. As he has recently highlighted, the issue of cybersecurity is

not a partisan one and I am glad that the chairman agrees with that, but is an issue on which Democrats and Republicans should be able to work together to come up with common sense solutions to help protect the American people.

Mr. Chairman, I look forward to working with you and the staff in a bipartisan way to update FISMA and pass comprehensive cybersecurity legislation in this Congress and I would ask unanimous consent that Mr. Langevin be a part of this hearing today.

[The prepared statement of Hon. Elijah E. Cummings follows:]

Opening Statement
Ranking Member Elijah E. Cummings

Hearing on "Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat"

July 7, 2011

In testimony before the House Intelligence Committee earlier this year, then-CIA Director Leon Panetta called cybersecurity "the battleground for the future." Our nation's critical infrastructure—including power distribution, water supply, telecommunications, and emergency services—have become increasingly dependent on computerized information systems to manage their operations and to process, maintain, and report essential information.

Our government's national defense and critical information systems are also becoming increasingly reliant on information technology systems and web-based transactions and services. Successful attacks on these systems threaten our troops, impair vital federal programs, and jeopardize the privacy of citizens whose personal information is maintained in government computer systems.

In the last Congress, Members of the House and Senate introduced at least 50 cybsersecurity-related bills to address these issues. Given the urgency and complexity of these challenges, Congressional leadership called on the Administration to help develop comprehensive cybersecurity legislation. On May 12th, the Obama Administration issued a legislative proposal that would significantly strengthen our ability to guard against cyber attacks. I applaud the President for his leadership on this issue and for creating a strong legislative framework to help Congress complete this important work.

For example, the Administration's proposal would make key changes to the Federal Information Security Management Act, or FISMA, including shifting to continuous monitoring and streamlined reporting for all federal systems. I supported similar legislation last year, and this Committee successfully reported out bipartisan legislation that would have achieved these goals, so I am glad to see the Administration's proposal has incorporated many of the improvements included in that legislation.

There are several provisions in the Administration's proposal that I would like to see strengthened. First, I hope we will consider the creation of a Senate-confirmable official with authority to set administration-wide cybersecurity policy. It is important that the official

responsible for implementing FISMA have the authority to task all civilian departments and agencies with implementation of the federal security standards.

The Administration's proposal also creates a framework to ensure that the federal government and private industry are working together to protect our critical infrastructure. Private industry owns approximately 85% of the nation's critical infrastructure, and the Administration's proposal allows critical infrastructure operators to develop their own frameworks for addressing cyber threats. However, while there is room for healthy debate, even industry agrees that some level of government oversight is necessary to protect the American public from the potentially devastating consequences of a cyber attack. At a recent hearing before the National Security Subcommittee, TechAmerica President Phil Bond testified that education and information-sharing alone are inadequate to protect critical infrastructure and that government "rules, regulations and requirements" are necessary to secure the nation's critical infrastructure.

Other parts of the Administration's proposal attempt to help consumers and companies by creating uniform reporting standards to address cyber attacks that result in breaches of personally identifiable consumer information. However, the proposal also would allow any entity to share with DHS personally identifiable information that otherwise could not be shared under existing law. I agree that we should encourage information-sharing between industry and government, but we also have to be careful that personally identifiable information is appropriately protected and shared with the government only when necessary.

Finally, I agree that law enforcement should have every tool necessary to go after hackers, but I am concerned that the imposition of mandatory minimum sentencing unduly interferes with judges' discretion to set appropriate penalties. I hope that future drafts of the legislation will not include this specific provision.

I would like to thank Chairman Issa for agreeing to include our distinguished colleague, Congressman Jim Langevin, in our hearing today. Jim has been a leader on cybersecurity for many years. As he recently highlighted, the issue of cybersecurity is not a partisan one, but is an issue on which Democrats and Republicans should be able to work together to come up with common sense solutions to help protect the American people.

Mr. Chairman, I look forward to working with you and your staff in a bipartisan manner to update FISMA and pass comprehensive cybersecurity legislation this Congress.

Chairman ISSA. I would join with you in that unanimous consent. I have served with Mr. Langevin on the Select Intelligence Committee and he has always been bipartisan.

Hearing no objection, so ordered.

Chairman ISSA. I would now recognize the chairman of the Subcommittee on National Security, Mr. Chaffetz, for his opening statement.

Mr. CHAFFETZ. Thank you, Mr. Chairman, and thanks for your leadership on this issue. It is certainly one of the most important topics.

The growing cyber threat is one of the greatest national security challenges facing the United States of America. It affects nearly every facet of the private and public sector and reaches deep into our personal lives.

On May 25, 2011, the Subcommittee on National Security, Homeland Defense and Foreign Operations conducted a hearing to examine the threat. Government officials testified alongside their private sector counterparts about the challenges that we face. Each gave us sobering overview of the threat and each communicated that the threat is real, is extremely dangerous and is persistent.

While digital connectivity has made life more convenient, it has exposed new vulnerabilities. Our personal computers are at risk, as well as cell phones, financial institutions, water and power infrastructure, State, local and Federal Government institutions. Bad actors continually scour the Web for our most sensitive information, social security numbers, credit card information, bank accounts, proprietary business information, defense and intelligence secrets, plans and intentions for our political and business leaders. They gain this information through advanced, persistent threats, social engineering and spear fishing.

Some hacks are carried out by individual actors and small-time crooks and other breaches are coordinated efforts by foreign governments. The most devastating attacks such as the Wiki leaks incident come from within. Each has the ability to inflict significant and irreparable harm.

Statistics indicate that corporations lose roughly $6 million per day when sites are down because of cyber attacks. The global economy loses approximately $86 billion per year. There is every indication that these costs will continue to increase. The President and members of the administration have publicly stated that the Federal Government is ill prepared to mitigate the threat.

The Department of Homeland Security testified "We cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis." Phillip Bond, the President of Tech America, testified "Cyber crime represents today's most prolific threat." It is no secret that the Federal Government's IT infrastructure has significant weaknesses. Across the executive branch, systems are outdated and technology is behind. Legal and regulatory frameworks are equally behind. The authorities, roles and responsibilities of Federal, State, local and private entities are unclear and insufficient to meet the threat.

The administration has submitted a proposal to remedy these shortfalls and this is a good first step. However, it will continue to need examination by this committee. It will also need extensive

input from the private sector which owns roughly 85 percent of the digital infrastructure. The solutions must be effective, efficient and allow all parties to be as nimble as the enemy.

I am confident the solutions put forth by this Congress, the administration and the private sector will yield exactly the results we need to protect our critical infrastructure. As a member of the House Cybersecurity Task Force and as the chairman of the National Security, Homeland Defense and Foreign Operations Subcommittee, I look forward to working toward an effective and efficient solution to the cyber threat.

I look forward to hearing from the witnesses, appreciate their expertise and your willingness to be here today.

I yield back, Mr. Chairman.

Chairman ISSA. I thank the gentleman.

We now recognize the ranking member of the subcommittee for his opening statement.

Mr. TIERNEY. Thank you, Mr. Chairman.

I want to thank you, Mr. Chairman, as well as Mr. Chaffetz, for putting this matter on the agenda and for taking it as seriously as we have in a bipartisan fashion. We are all familiar with the various incidents that have happened, including earlier this month when CitiGroup revealed that hackers had stolen personal information from more than 200,000 credit card holders. This was one of the larger direct attacks on a major bank ever reported, but it is not singular in its occurrence. Thieves obtained customer names, card numbers, addresses and email information. The unfortunate part is it took the company, as it does too many companies, over a month to notify all the customers of the breach, so that sheds some light on the need for stringent reporting requirements for breaches of personal information.

It highlights the fact that banks and some other companies are focused on fraud and reducing fraud but they also have to be concerned about the prevention of data theft itself and the impact it can have on the consumer. In fact, the data theft arguably is of less cost to the entities than is the fact of consumer information getting out. The question is where the incentives really lie in terms of making people do what they need to do to meet the standards to prevent this from happening in the first place.

I join others in applauding the administration for creating a national data breach regulation system that will ensure that consumers learn about the data breaches as soon as possible. I applaud their efforts to encourage companies to share data about cyber attacks and the Federal Government to improve defenses against these types of attacks.

When we hear about all of the incidents that occur, I think it becomes clear that we need some standards. Of course the issue then becomes if everyone doesn't adhere to those standards, how well protected are those that actually do. That is where we get into at what point does it become too costly to adhere to the standards, and if some play and others don't, do we just leave everyone exposed. I think that is the critical thing I would ask our witnesses to hone in on today and help us with because it is going to take an effort from everyone, the companies, the government, and the consumers.

We have to be careful when we start talking about immunization. I know there may be a place for it but I am concerned it is going to put the incentives in the wrong place and take away from some incentive to really focus on the need to go after stopping these data attacks from happening in the first place and from having people comply. I would like to hear a lot of discussion on that.

I don't want to see us take the wrong approach and sort of immunize people, then get lax and think, I don't have to play, I don't want to spend that money, and I don't want to be responsible for it. I think we have to talk about people being accountable, particularly those that will profit from it, but we have to reasonable and understand that in some places there may be a need for incentives that draws in everyone because of the expense involved.

I thank our witnesses for being here today, and the chairman for raising this issue.

I would like to yield the balance of my time to the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. I would like to thank the gentleman for yielding. I would also like to thank Chairman Issa and Ranking Member Cummings for allowing me to sit in on today's hearing.

Mr. Chairman, I deeply appreciate the time and attention you and this committee have paid to this issue. As a member of both the House Armed Services Committee and the House Intelligence Committee, as co-creator of the Bipartisan Cybersecurity Caucus, and as someone who has spent many years on this issue, I have a deep appreciation for the challenges we face in the field of cybersecurity. I echo the comments and concerns that you, Mr. Chairman, the ranking member and others have raised today.

Earlier this year, I introduced legislation to strengthen the outdated Federal Information Security Management Act. This language was developed last year by my friend and former colleague, Representative Diane Watson, as well as this committee and that legislation was passed by this committee.

Unfortunately, due to concerns over cost estimates, we were unable to pass these provisions as an amendment to the Fiscal Year 2012 Defense Authorization bill. However, I know that members of this committee are committed to working on this problem and I am heartened to see the administration coming forward in this area as well.

With that, again I deeply appreciate the opportunity to join you today and look forward to the testimony of our witnesses.

I yield back.

Chairman ISSA. I thank the gentleman.

Members may have 7 days to submit opening statements and extraneous materials for the record.

We now recognize our panel of witnesses. Mr. Greg Schaffer is the Acting Deputy Assistant Secretary of the National Protection and Programs Directorate of the U.S. Department of Homeland Security. Mr. James A. Baker is Associate Deputy Attorney General at the Department of Justice. Mr. Robert J. Butler is the Deputy Assistant Secretary for Cyber Policy at the U.S. Department of Defense. Mr. Ari Schwartz is the Senior Internet Policy Advisor at the National Institute of Standards and Technology at the Department of Commerce.

Welcome to all of you.

Pursuant to committee rules, would you please rise to take the oath. Please raise your right hands.

[Witnesses sworn.]

Chairman ISSA. Let the record reflect that the witnesses answered in the affirmative.

Some of you are returning heroes, so you know this drill. In order to allow enough time, your entire statements as presented will be placed in the record. We would ask you to summarize in any way you choose but keep it within 5 minutes. When you see the yellow light go on, it is not shameful to stop sooner than when the red comes on, but in all cases, please wrap up by the time the red comes on.

With that, Mr. Schaffer.

STATEMENTS OF GREG SCHAFER, ACTING DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY; JAMES A. BAKER, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE; ROBERT J. BUTLER, DEPUTY ASSISTANT SECRETARY FOR CYBER POLICY, U.S. DEPARTMENT OF DEFENSE; AND ARI SCHWARTZ, SENIOR INTERNET POLICY ADVISOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

STATEMENT OF GREG SCHAFFER

Mr. SCHAFFER. Thank you, Chairman Issa, Ranking Member Cummings and members of the committee. It is an honor to appear before you today.

I know that the committee has already had a number of hearings and briefings on this topic, so I will briefly summarize the current state of affairs and the impetus for the legislative proposal that you have from the administration today.

There is no security issue facing our Nation that is more pressing than cybersecurity. The vulnerability of our networks is an issue of national security, of homeland security and of economic security. The reality is that the United States is increasingly confronted by a dangerous cyber environment where threats are more targeted, are more sophisticated and more serious than they have ever been before.

Our adversaries are stealing sensitive information and intellectual property from both government and private sector networks, comprising our competitive economic advantage and jeopardizing individual privacy.

More disturbing, we also know that our adversaries are also capable of targeting elements of our critical infrastructure to disrupt, dismantle or destroy the systems upon which we depend every day. As the electric grid, major financial institutions and mass transportation and other critical infrastructure elements attach to the networks, they can become vulnerable to cyber attack.

This is not conjecture, it is reality. Hackers probe critical infrastructure companies on a daily basis. The status quo is simply unacceptable and we believe a solution can be found if we work together. Today's threats require engagement of our entire society

from government to the private sector to the individual citizen. For that reason, the administration has recently sent a legislative proposal to Congress that focuses on clarifying cybersecurity authorities and collaborating with the private sector.

I will briefly talk about portions of the proposal and the rest of the panel will address some of the other portions.

With respect to protecting the Federal Government, the proposal clarifies DHS' leadership role in civilian cybersecurity consistent with the last administration's CNCI, Comprehensive National Cybersecurity Initiative proposals. First, the proposal solidifies that the Department of Homeland Security's responsibility for leading and protecting Federal civilian networks and ensure that our authorities are commensurate with our responsibilities.

DHS provides a number of services to departments and agencies today and sometimes the lack of clear legal authority slows us down in doing that and this proposal will clarify our legal authority. It will also modernize, as noted, the Federal Information Security Management Act [FISMA], to focus on continuous monitoring and operational risk reduction rather than a paper-based compliance reporting regime.

We believe that the transfer of the FISMA oversight responsibilities from OMB to DHS, which started under an OMB memorandum last year, would just be solidified by the proposal and it would enhance by consolidating the policy development, oversight and operational expertise within one agency.

Under personnel authority, the proposal would give DHS the ability to attract and retain cybersecurity professionals in an environment that is extraordinarily competitive by extending to DHS, DOD's current cybersecurity personnel authorities and create an exchange program for cybersecurity experts to move between government and the private sector.

To protect critical infrastructure, we have a combination of voluntary and mandatory programs to focus on public/private partnerships. The administration proposal clarifies DHS' authority provide a range of voluntary assistance to a requesting private sector company, State or local government. It clarifies the type of assistance that DHS will be able to provide, including alerts, warnings, risk assessments, onsite technical support and incident response.

Organizations that suffer attacks often ask the Federal Government to assist, but the lack of clear statutory authority and a framework sometimes slows down that process and we think this will accelerate it.

From an information sharing perspective, we will remove the barriers to sharing cybersecurity between industry and government. It will allow industry partners to share with us that which they learn from their networks without having to go through a series of legal conversations in order to ensure themselves that they are allowed to share. That will eliminate delays sometimes of days, sometimes of weeks, before we can get data that can be leveraged to help the entire community.

Under the mandatory provisions of the proposal, we would leverage our existing and consistent partnership with the private sector to develop a set of frameworks that would be used to reduce risk. We would work with the private sector to identify the risk, we

would work with the private sector to identify the frameworks and then the private sector would develop plans to actually implement and reduce the risk within their organizations. It is a proposal that really works with industry and leverages industry's expertise more than thinking that the government has all the answers.

We look forward to working with you. This is a proposal. It is not the end of the discussion but the beginning of the discussion. We look forward to working with the committee on a going forward basis.

[The prepared statement of Mr. Schaffer follows:]

Statement for the Record
Of

Greg Schaffer
Acting Deputy Undersecretary
National Protection and Programs Directorate
Department of Homeland Security

James A. Baker
Associate Deputy Attorney General
Department of Justice

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

Before the
House Oversight and Government Reform Committee
United States House of Representatives
Washington, DC

July 7, 2011

Introduction

Chairman Issa, Ranking Member Cummings, 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.

Chairman ISSA. Thank you.
Mr. Baker.

STATEMENT OF JAMES A. BAKER

Mr. BAKER. Good morning, Mr. Chairman, Ranking Member Cummings and members of the committee. Thank you for the opportunity to testify on behalf of the Department of Justice today regarding the administration's cyber legislation proposal.

Because of the short time I have this morning, rather than commenting further on the cyber threat, which as the committee is well aware, is very serious, I will focus my remarks on two portions of the administration's proposal intended to enhance our ability to protect the American people from cyber crime.

First is data breach notification. Data breaches frequently involve the compromise of sensitive, personal information and expose consumers to identity theft and other crimes. Right now, there are 47 different State laws requiring companies to report data breaches in different situations and through different mechanisms.

The administration's data breach proposal would replace those 47 State laws with a single national standard, applicable to all entities that meet the minimum threshold as set forth in the proposal. If enacted into law, this proposal would better ensure that companies notify customers promptly when sensitive, personally identifiable information is compromised and that they inform consumers about what they can do to protect themselves.

The proposal would empower the Federal Trade Commission to enforce the reporting requirements. It would also establish rules about what must be reported to law enforcement agencies when there is a significant intrusion so that, for example, the FBI and the U.S. Secret Service can work quickly to identify the culprit and protect others from being victimized.

The national standard would also make compliance easier for industry, we believe, which currently has the burden of operating under the patchwork of different State laws that I mentioned a moment ago.

Second, the administration's proposal includes a handful of changes to 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 will make it clearly unlawful to damage or shut down a computer system that manages or controls a critical infrastructure and would establish minimum sentence requirements for such activities. This narrow focused proposal is intended to provide strong deterrence to this class of very serious, potentially life threatening crimes.

Moreover, because cyber crime has become big business for organized crime groups, the administration's proposal would make it clear that the Racketeering Influenced and Corrupt Organizations Act applies to computer crimes. Also, the proposal would harmonize the sentences and penalties in the Computer Fraud and Abuse Act with other similar laws.

For example, acts of wire fraud in the United States carry a maximum penalty of 20 years in prison but violations of the Com-

puter Fraud and Abuse Act involving very similar behavior carry a maximum of only 5 years.

Thank you, Mr. Chairman and members of the committee. I look forward to your questions on this important topic.

Chairman ISSA. Thank you.

Mr. Butler.

STATEMENT OF ROBERT J. BUTLER

Mr. BUTLER. Thank you, Mr. Chairman, Ranking Member Cummings and distinguished members of the committee. It truly is a pleasure to appear before you today.

On behalf of the Department of Defense, we are aware, of course, and are working against the persistent threat. The DOD is reliant on a large portion of the Nation's critical infrastructure such as power generation, transportation, telecommunications and of course, the defense industrial base to defend the Nation and perform those missions assigned to and expected of DOD.

The most important aspect of the Nation's critical infrastructure protection, from our standpoint, is the recognition that no one person or agency can protect the Nation from this advanced, persistent threat that we have been discussing. Rather, it will require a whole of government approach, necessitating many different Federal agencies, State governments and the private sector to work together. This legislation is an important step in that direction.

It criminalizes the damage to critical infrastructure systems, breaks down barriers to information sharing so that stakeholders can communicate effectively. It engages the private sector as valuable stakeholders and strengthens the ability of the Department of Homeland Security to lead the executive branch in defending the Nation against the very real cyber threat.

Importantly, this legislation accomplishes all of the above while respecting the values of freedom and ensuring the protection of privacy and civil liberties that we cherish in this country.

The Department of Defense has an important role in this Nation's cybersecurity such as protecting our military networks and national security systems while providing support and technical assistance to the Department of Homeland Security in carrying out other protection issues regarding critical infrastructure.

DOD has and will continue to work hand in hand with Homeland Security, Commerce, Justice and the other departments, along with the private sector in countering cyber threats and protecting our Nation's critical infrastructure. Further, the administration's legislative proposal allows DHS to leverage DOD's practices in hiring and personnel exchange programs as well as reinforcing the complementary and continuing defense role in providing information systems controls of defense and national security systems under the Federal Information Security and Management Act.

We do look forward to working with Congress to ensure the executive branch has the appropriate authorities for cybersecurity and improving the overall security and safety of our Nation.

I would like to close by noting by that while the work of defending the Nation is never done, this legislation will greatly help the U.S. Government close the gap between us and those who would

want to do us harm. As I noted before, the threat is constantly evolving and we must evolve to meet it.

The Department of Defense is ready to play its role in meeting this challenge and to work with the rest of government to protect the citizens and resources of the United States.

Thank you.

Chairman ISSA. Thank you.

Mr. Schwartz.

STATEMENT OF ARI SCHWARTZ

Mr. SCHWARTZ. Chairman Issa, Ranking Member Cummings and members of the committee, thank you having me today to testify on behalf of the Department of Commerce on the administration's cybersecurity legislative proposal.

The main goal of this proposal is to maximize the country's effectiveness in protecting the security of key critical infrastructure networks and the systems that rely on the Internet, while also minimizing regulatory burdens on the entities that it covers and protecting the privacy and civil liberties of the public. To accomplish this balance, we focused on building transparency throughout the process that rely heavily on public/private partnerships.

I will be addressing four important pieces of the proposal: creating security plans for covered critical infrastructure; protecting Federal systems; protecting data breach reporting, and privacy protection.

One important theme of the proposal is accountability through disclosure. In requiring creating of security plans, the administration is promoting use of private sector expertise and innovation over top down government 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 NIST to work with them to help create security frameworks.

There would be strong incentive for both industry to build effective frameworks and for DHS to improve those created by industry. The entities involved would want the certainty of knowing their approach has been approved and the Federal Government will benefit from knowing it will not need to invest in the resource intensive approach or development of government-mandated frameworks unless industry fails to act.

Covered critical infrastructure firms and their executives will then have to sign off on their cybersecurity plans, subject them to performance evaluations and disclose them in their annual reports.

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

The proposal also clarifies the 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 then use these standards as a basis for binding directives and memoranda it issues to the Federal agencies.

A working partnership between Commerce, NIST and DHS will be important to ensure that agencies received information security requirements that are developed with appropriate technical operational and policy expertise.

On data breach reporting, the administration has learned a great deal from the States selecting and augmenting the strategies and practices we feel most effective to protect security and privacy. The legislation will help build certainty and trust in the marketplace by making it easy for consumers to understand the data breach notices they receive, why they are receiving them and as a result, they will better be able to take appropriate action.

As Secretary Locke and others at the Commerce Department have heard from many companies and different industries, including responses to our Notice of Inquiry last year, a nationwide standard for data breach notification will make compliance much easier for the wide range of businesses 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 by and shared with the government for cybersecurity purposes.

This framework would be created in consultation with privacy and civil liberties experts and the Attorney General, subject to regular reports to Congress and overseen by the Independent Privacy and Civil Liberties Oversight Board. Governmental violations of this framework will be subject to criminal and financial penalties.

Thank you again for holding this important hearing and I look forward to your questions.

Chairman ISSA. Thank you.

I will now recognize myself for a first round of questions.

Just a comment, Mr. Schwartz. One of the challenges I face, as I am a Californian, I know that when we harmonize a 50-State solution, it is 50 States plus California's add-on, so I look forward to working on this legislation so that it not be 49 States plus California as it has been in so many other areas. I agree that we have to get to an interstate commerce, genuine compact with all States. Hopefully, we can find a constitutional way to bind all States so that there is a one for all and all for one law.

I have a couple of questions. Mr. Baker, I looked through your background and you worked here for the fights on FISMA but Mr. Tierney referred to it and Mr. Schaffer, with his background, very much knows its history.

When we asked communications companies to give us information after 9/11, they found themselves embroiled in lawsuits because of it. One of the challenges in the proposal is that it presumes there will be this free flow of information one way and only

one way which is from the private sector to government, but it doesn't specify the actual protections for those who give what is otherwise not the requirement to give, at least federally.

Have you worked out how you are going to propose keeping the plaintiffs' trial bar out of the businesses each and every time something goes wrong for these companies that have been reporting or if there is, effectively, a leak of private information from the government that is then traced back to a private company who delivered? I understand there is a mandatory part and there is implied immunity but on the voluntary part?

Mr. BAKER. Thank you, Mr. Chairman.

I think on the voluntary part there is an immunity provision in the proposal and that would apply to the voluntary sharing so that if they shared the information and then somehow found themselves embroiled in a lawsuit, they could rely on that provision. We think that is how it would come out. At the end of the day, a judge would have to rule on whether it applied or not and if it was proper.

Chairman ISSA. With AT&T and the others, that was exactly the problem. The Federal Government had a need to make sure that information not be made public. As a result, the companies were unable to properly defend themselves. We have been down the road of an implied immunity versus and explicit one and also one of the concerns, and Mr. Tierney isn't here but I will share perhaps what is one of this concerns, we don't want somebody to voluntarily deliver information in order to gain immunity they otherwise wouldn't have.

Have you looked at that side of the equation? Not from the standpoint of a judge will decide, but that our two bodies will write it in a way in which it is predictable, what the outcome would be?

Mr. BAKER. Yes, we are very aware of that concern and we have tried to factor that into our thinking very much. That is why I think you see the immunity provision has sort of two parts to it. One is appropriate sharing pursuant to the subtitle that would be this provision. The other is where you have a good faith belief that your sharing is lawful.

If you have a bad faith belief that you are sharing, you are sharing for some ulterior purpose, that would not be covered, but if you are sharing within the confines of the subtitle or sharing in good faith, then you would be protected.

Chairman ISSA. Mr. Langevin and I both worked on this sometime ago. Having been there, if the government asks, one might say that if you answer that is a good faith belief. That is exactly where George W. Bush and his Attorney General found themselves sideways. They had clearly asked, industry had answered and then there was a debate about whether or not that was covered.

You may want to look at that as we go through the drafting process to make sure that effectively if government, whatever government, thinks it is legal and they ask the question, that should be, in my opinion, at least, an explicit immunity because even though it is voluntary, I think all of us on both sides of the dais know that a voluntary question asked by a governing body has a certain amount of you will answer gravitas.

Mr. Schaffer, only a few weeks ago, we thought this was going to come out as recommendations and it came out as a proposal. Is

that because you felt you were closer to, if you will, final legislative language or was it simply easier to put it into this format? We were a little surprised when it came out in legislative format.

Mr. SCHAFFER. Thank you, Mr. Chairman.

I can't speak to exactly the decision process to bring it out in this way. I can say that in the development of the various pieces of the proposal, there was legislative language prepared as we transmitted it and the decision was made that would be the easiest way to bring those ideas forward.

Chairman ISSA. As I recognize the ranking member, the reason I asked that was that our intention is to bring a series of private sector individuals both in a formal fashion and in a less formal fashion, so that we can glean their input. Our understanding is this has been government formatted and there has been no formal outreach to the private sector.

That is one of our concerns. All the opening statements talked about the 85/15. Our goal is, now that this in a proposed language, to begin communicating with the stakeholders and the private sector, and quite frankly, also some of the State representatives. Hopefully we can share in that.

I recognize the ranking member for his round of questions.

Mr. CUMMINGS. Thank you very much.

In the wake of 9/11, new attention been focused on the significance of information sharing as a matter of national security. The 9/11 Commission report says the biggest impediment to all source analysis to a great likelihood of connecting the dots is the human or systemic resistance to sharing information. They said something. There is widespread consensus on the need for more robust information sharing from the private sector to the government and vice versa to better protect our cyber networks and critical infrastructure.

To all the panelists, how do we overcome this systemic resistance to achieving this goal? Mr. Schaffer.

Mr. SCHAFFER. Thank you, sir.

I think the proposal is designed to eliminate some of the barriers that we see to information sharing. One of the challenges we have consistently when an entity has information they believe the government should know and would help the broader community to protect both government and the private sector, is there they are not sure what they are allowed to share and what they are not allowed to share. They are not sure whether there is some legal provision somewhere that is going to get them into hot water if they provide the information on an expedited basis to the government.

This mention of it being one way sharing, our goal when we receive the information at DHS is to use that information and distribute the pieces that can be used to defend networks as quickly as possible to the broadest audience.

The provision in the proposal that provides, notwithstanding any other law, you can provide that information and there is immunity for the sharing of that information if it is for a legitimate cybersecurity purpose, we think will enhance the ability of private sector entities to give information to the government.

Mr. CUMMINGS. Mr. Baker.

Mr. BAKER. Thank you, sir.

I think that the key, as Mr. Schaffer touched on, is clarity in the law. I think we need language that clearly would authorize the sharing. We need clear limitations on that, in other words privacy protections in particular. You need a clear immunity provision, as I was just discussing with the chairman a few minutes, and then you also need, what we have heard, clear exemptions from FOIA as well because when folks share information with the government, they become concerned it is going to be discoverable, if you will, under FOIA.

I think the key is clarity so that they don't have to search through the Federal Code to determine what provisions they may or not be violating if they were to share this information. I think clear language that is straight forward is the main objective.

Mr. CUMMINGS. Mr. Butler or Mr. Schwartz, do you have anything in addition to what they just said? I don't want us repeating each other.

Mr. BUTLER. I support what they described. Beyond the legislation, I was going back to the intent of the post-9/11 Commission. I think we have been working on is building relationships. You saw that within the Department of Defense, the Department of Homeland Security building MOAs, building collaboration and second, planning together, the National Cyber Incidence Response Plan. That developmental activity is really enabling information sharing in new and different ways and exercising together, cyberwatch and those kinds of exercises really help us to build the connective tissue to enable an information sharing approach.

Mr. SCHWARTZ. I will just briefly say that we have made large strides in terms of getting greater information sharing. I think you gave an excellent overview of all the difficulties. We tried to address some of those in sharing with government in the proposal. We are certainly open to broader discussions of other kinds of sharing and other ways of addressing these issues without unduly affecting privacy and other issues.

Mr. CUMMINGS. One of the things, Mr. Butler, and some of the others may be able to answer this, in the Naval Academy, we made this a top priority. In our last meeting, we were discussing how while the Naval Academy is moving forward with phenomenal speed now that we need to get this kind of teaching to private colleges. We were trying to figure out how we could take the Naval Academy's curriculum and then spread it.

We were very concerned that we are not preparing enough of our young people to deal with this threat. I am just wondering what we are doing with regard to that because we can create all the rules we want, but if we don't have folks who are equipped to address this, we have major problems. We have become basically a defenseless nation. You are all pointing out how urgent the situation is, what are we doing in that regard?

Mr. BUTLER. From the DOD perspective, Secretary Gates made it a top priority in terms of next gen work force education for defense and the national security base so it is the Academy at Annapolis and certainly the other academies. We have a fairly large program through the Department of Defense on information assurance which reaches colleges around the United States, working with

them on curriculum development as well as internships and scholarships for students.

We build on that with the Cyber Patriot Program where we are involved with high school and junior high students. We support the National Cyber Collegiate Defense competitions. More than competitions, they are actually coaching and mentoring programs. There are continuous education outreach programs to allow us to help young people understand what we are faced with and to actually cast a dream for them to get involved.

Mr. CUMMINGS. Thank you very much.

Mr. CHAFFETZ [presiding]. I will now recognize myself for 5 minutes.

One of the emergency national security concerns is that you have software infrastructure, hardware, other things that are built overseas that comes to the United States with items that are already embedded in them by the time they get here. This obviously poses security and intellectual property risks. Is any of this happening, Mr. Schaffer, and what are we going to do to fight this?

Mr. SCHAFFER. Clearly supply chain risk management is an issue that the administration is focused on. Homeland Security is working with partners at the table.

Mr. CHAFFETZ. How are they focused on it? Is this happening?

Mr. SCHAFFER. Whether or not there are specific examples of insertions is something I would rather talk about——

Mr. CHAFFETZ. I think you would rather not. It is just a yes or no question. Is this happening or not?

Mr. SCHAFFER. We believe that there is significant risk in the area of supply chain.

Mr. CHAFFETZ. Is it happening, to the best of your knowledge? I am sorry. I thought I threw you a softball to begin with. Is this happening or not?

Mr. SCHAFFER. I missed the very beginning of the question and the wording that you gave me and I apologize. I don't want to get this wrong. Can you rephrase for me?

Mr. CHAFFETZ. Are you aware of any component software/hardware coming to the United States of America that have security risks already embedded into those components?

Mr. SCHAFFER. I am aware there have been instances where that has happened.

Mr. CHAFFETZ. What is Homeland Security doing about this? What can we do about this?

Mr. SCHAFFER. This is one of the most complicated and difficult challenges that we have. The range of issues goes to the fact that there are foreign components in many U.S.-manufactured devices.

Mr. CHAFFETZ. Yes. That is the obvious. Go faster, I only have 5 minutes here. There are many foreign components in our materials, yes. I got it.

Mr. SCHAFFER. There is a task force that DHS and DOD co-chair to look at these issues with goals to identify short term mitigation strategies and to also make sure that we have capability for maintaining U.S. manufacturing capability over the long term and are in a position to ensure that the critical infrastructure pieces have what we need.

Mr. CHAFFETZ. It is terribly complicated, I understand it is difficult, but the concern is that it is happening and probably happening on a more frequent basis than most people recognize. These things are embedded in devices and software and people don't know that. It is very difficult to detect.

Let me move on and stick with you, Mr. Schaffer, on this. There is a lot of discussion here about private to public having to report to the government. How much did the government—the White House, Homeland Security and others—work with the private sector? The numbers are pretty big, upwards of 85 percent of the infrastructure that is used is from the private sector, the networks used are run by the private sector, but there is a lot of concern that the private sector really wasn't at the table when this was developed. Were they at the table and how much so?

Mr. SCHAFFER. With respect to the proposal you have before you, as we said, we think this is the beginning of the conversation. It was developed and informed by our long term and existing relationships with the private sector. Frankly, I have spent the vast majority of my career in the private sector working as a chief information security officer and as a consultant to large corporations.

We built this proposal based on what we have learned through the National Infrastructure Protection Plan process, our relationships with each of the sectors, the sector coordinating councils, the ISACs and others. I believe this proposal is designed to give the private sector tremendous input into the process both in identifying the risk, identifying the frameworks, building their own plans.

This doesn't prescribe specific technologies they need to use, it doesn't give them a mandate to do this in any certain way. It gives them an opportunity to participate in developing a regime that will allow us to reduce risk.

Mr. SCHWARTZ. Mr. Chairman, just briefly. The Department of Commerce actually had a Notice of Inquiry last summer that addressed many of the pieces that are now in this legislative proposal that were informed by input from the private sector, so at the beginning, there was some informed piece that came from this.

Mr. CHAFFETZ. I guess one of the concerns I have moving forward, for further discussion, one of the shortcomings I see is how do we take it from the public realm and inform the private sector? It seems to be very much a one way street. It needs to be back and forth. I see you are all shaking your heads, I hope there is concurrence on this. We will have to work on the specific language and how that information would flow because it does need to be communicated back and forth.

I have lots more questions but my time has expired. With that, we will now recognize the gentleman from Tennessee, Mr. DesJarlais for 5 minutes.

Mr. DESJARLAIS. Thank you, Mr. Chairman. Thank you, gentlemen.

A growing threat in both the public and private sector information systems is cyber attacks from foreign governments or organizations mostly aligned with them. Cyber attacks certainly are not exclusive to the United States, other countries have experienced such attacks. At what point do cyber attacks carried out by foreign gov-

ernments become an act of war or what some refer to as cyber warfare against another nation? I would open that to everyone.

Mr. BAKER. That is a legally difficult question to answer but certainly acts that would be equivalent in their effects to a kinetic attack on the United States would fall within the category I think you are talking about there. If you look at the effects that were equivalent to a kinetic attack, that would be an act of war.

Mr. DESJARLAIS. Have we developed any effective means of identifying who the actors or players in these attacks are?

Mr. BAKER. Attribution is very difficult in this area. That is challenging. It doesn't mean it can't be done, but it is challenging. I would defer to my colleagues if they want to add something on that.

Mr. BUTLER. We continue to evolve with the technology to help us with attribution and tactics, techniques and procedures but right now, it is a fairly intensive forensic analysis process that we go through to attribute to actors.

Mr. DESJARLAIS. Both public and private sectors are deeply interwoven and dependent upon each other for their operations and functionality. For example, telecommunications and transportation are heavily dependent on the power grid for operations and vice versa. Does our current Internet or communications infrastructure have enough redundancy built in to ensure that we could survive a catastrophic attack on its physical or technical assets, Mr. Schaffer?

Mr. SCHAFFER. There have been numerous attempts to look at that question through risk analysis by various sectors including the IT sector, the calm sector and the belief is there is a significant amount of resiliency within the network. Certainly the Internet was built with resiliency in mind and the ability to route around various types of problems.

On any given day with any particular kind of attack, it is hard to say whether you will have enough resiliency in that particular place but I do think the architecture of the system is designed to be quite resilient. There are certain pieces of the puzzle that obviously need more security and that is where I think we are with the legislative proposal today.

Mr. DESJARLAIS. Does the Federal Government have an effective defensive posture to ensure that attacks on private sector networks or infrastructure can be isolated with little damage to its own assets?

Mr. SCHAFFER. I would say that we are very much, both industry and government, dependent on one another in a variety of ways. It would be very difficult to isolate the government from the critical infrastructure pieces that are provided by industry. As noted, they own a substantial portion of that infrastructure.

Mr. DESJARLAIS. There have been a number of economic estimates regarding the cost of a major cyber attack on the economy. Are there consistent, reliable numbers that tell us how much cyber crime or cyber attacks cost the United States each year?

Mr. SCHAFFER. There are a wide range of estimates. I don't know there is a single, consistent, across the board way to estimate what those costs would be. Over the last several years we have seen we are attaching more and more of our critical infrastructure to the

Internet for the efficiencies that it can bring. That adds to the potential for damage if those systems are compromised. I am not aware of a single metric that can be used to identify how much damage is within the art of the possible.

Mr. DESJARLAIS. Where are the most significant weaknesses in our IT supply chain?

Mr. SCHAFFER. I don't know that I can identify the most significant weaknesses within the supply chain. As I said, the supply chain issues are increasingly complex because we do have a global economy in which our products and equipment is installed and embedded in foreign product, foreign product is installed and embedded in our product, and the need to have appropriate processes to address risk and manage ways of identifying where there might have been a compromise to the system is what we focus on in terms of programmatics at the Department.

Mr. DESJARLAIS. Thank you all. I yield back.

Mr. CHAFFETZ. The gentleman yields. I now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman, and welcome to the panel.

I certainly agree that cybersecurity is perhaps the largest growing single threat both to American infrastructure and to national security. The number of cybersecurity incidents reported by Federal agencies has increased from 5,000 to 41,000 over the last 5 years. One of the concerns I have is that when we had hearings on this subject a few years ago in this committee, we took testimony from a lot of Federal agency heads who focused on the part of FISMA that requires education, training and awareness. They could check off that box and say 80 percent of our work force is trained.

When you ask the question, are threats going up or down, they were going up, of course, and are successful, hacking attempts or cybersecurity threats going up or down, that also was going up. I would ask first, Mr. Schaffer, and anyone else on the panel, are we really working with the right metrics here on the subject of cybersecurity with Federal agencies or are we measuring the easy to measure?

Second, what kind of uniformity is there across dozens of Federal agencies to take the proper measures to protect the systems in place understanding the differentiation among those agencies?

Mr. SCHAFFER. Thank you for the question. Indeed, the reason you see this legislative proposal around FISMA is we recognize there needs to be a change in the way FISMA works. Even without the legislation in place, we have taken an approach that is much more aggressive since the Department has been asked to take on more responsibility.

We are meeting with the department CIOs to sit down and walk through all of the various requirements, not just the training requirements, but all of the requirements that currently exist and talk about how to prioritize those things that really matter and that will reduce operational risk.

Our approach is to get to continuous monitoring so we aren't reporting annually with a piece of paper what is happening on someone's network, which as you know is outdated before the paper is

written, but are seeing what is happening on those networks, can correlate that data with what we are seeing from our intrusion detection and intrusion prevention technology at DHS and actually work with the departments and agencies to reduce the risk they are seeing in terms of the kind of attack experience they have on a daily basis.

Mr. SCHWARTZ. You asked very good and extremely important questions.

Mr. CONNOLLY. I hope the chairman heard that, very good and extremely important questions, Mr. Chaffetz.

Mr. SCHWARTZ. In terms of what we are measuring, one of the main problems we have seen is inspectors general have looked at the controls that have been put in place as a checklist rather than trying to get at the main set of problems out there. One of the things we try to do in the administration proposal is to provide more flexibility in the structure so that the inspector general will look at what is important for that particular agency.

At the same time as Mr. Schaffer suggested, we try to increase automation through continuous monitoring through other means that we have a better standard across all different agencies. That doesn't mean we can stop other means of looking at the best practices and the controls that are in place, but we do need to do a better job of making sure we have the right controls for the right agency. We think the administration proposal does that with changes to FISMA.

Mr. BUTLER. I would just add what we see in the Department of Defense I think is reflective of our general sense of where we need to go with metrics. We look at technology, tactics, techniques and procedures and people in an integrated way, so as we work to harden networks and improve our cyber hygiene practices, we also look at proactive defense measures that we continue to incorporate in those areas.

Continuous red teaming, testing against what we are doing helps us to update the metrics. As we have stood up, organizational structures like Cyber Command and others, we are moving more and more toward what others are talking about with a continuous monitoring mode that builds beyond FISMA and helps us to ensure what anomalies we are missing that potentially could be problems down the road.

Mr. CONNOLLY. Is there a mechanism within the Federal Government for exchanging best practices, experiences, tapping into the private sector expertise and the like? Is there some kind of forum, formal or informal, that does that?

Mr. SCHAFFER. Actually, there is. One of the things DHS sponsors is something called the Cross Sector Cybersecurity Working Group. This represents the critical infrastructure, 18 sector cybersecurity resources and gives them an opportunity to work together to bring the knowledge that one sector may have learned to the other sectors. It is one of the goals of the program to make sure that wherever we see an issue we can get that information out to the entire community.

Mr. CONNOLLY. Mr. Chairman, I know my time is up but I think that is very important point. We want to break down the stove-

pipes here so that we are sharing experience and intelligence across agencies to try to deter the threat.

Thank you very much.

Mr. CHAFFETZ. Thank you. The gentleman yields.

We will now recognize the gentleman from Texas, Mr. Farenthold, for 5 minutes.

Mr. FARENTHOLD. Mr. Schaffer, I think you used the term you are seeing attacks every single day, 41,000 attacks reported. We see this growing at an incredible rate. I am very much afraid that we have a problem here that is going to be very difficult and very expensive to fix, both within the government and within the private sector.

Correct me if I am wrong. We have a wide variety of threats coming from everywhere. We have nation states as possible offenders, terrorists, criminals, industrial espionage, I guess we will call them hobby hackers, a wide variety of people intruding into computer systems. I don't think a day goes by that I don't have to install some sort of security update on my computer.

I guess my question is, I guess we need to take a multi-tiered approach. Where do you see the focus needs to be? Do we need to be focusing more on hardening systems to attack, do we need to be focusing on prosecutions? Where is the balance we will get the most bang for the buck?

Mr. SCHAFFER. Thank you for the question Congressman. Frankly, I think we need to do it all. This is not a single solution problem, it is not a problem that can be solved by any one entity, it can't be solved by government alone, it can't be solved by industry alone, it can't be solved by a single technology. This is going to take a whole of government effort, it is going to take a whole of society effort, right down to individuals who need to apply the patches and the virus updates to their machines.

The ecosystem was built in a way that allowed us to take advantage of moving very fast but the security pieces have been, for the large measure, bolted on after the fact. We are trying now to fix those issues but I do think it is going to require us to build better perimeters, apply those patches everywhere on all of the systems, update those systems to the best technology and do this vigilantly in all cases.

Mr. FARENTHOLD. I guess I will open this up to the rest of the panel. I don't know who might be the expert on this or if anyone has any ideas. Does anyone have a clue what this is going to cost in some reasonable term that we can understand? The price of a computer now is $500, an average piece of software, depending on what is? Percentage-wise, how much is it going to raise the cost of computing to do this?

Mr. SCHAFFER. While I can't say how much it will cost to do this, what I think has been said repeatedly is how much it is costing us for not having done it. The cost to our society, all that we are spending on trying to chase this problem, deal with the intrusions when they occur, the intellectual property loss that is going to hit us in terms of our economic competitiveness at a later point in time, those costs are also very hard to estimate but we know they are large.

Mr. FARENTHOLD. Where do you balance it between what the government spends and what the private sector spends and businesses and what I have to spend in order to surf the Internet at home?

Mr. SCHAFFER. What I think this proposal does that we never had before is a way to design for critical infrastructure a regime that actually allows for a standard of care to be developed for clear frameworks to be laid out that industry agrees with, they understand the risks, they know what they need to do in order to meet those risks and make them go down. If we do that, I think the markets will develop to produce the products that will make that easier and less expensive if everyone is working to that end.

Mr. FARENTHOLD. I only have a minute left and I want to hit on one other topic. I am deeply concerned that as you see increased cooperation between the government and the private sector, my data stored out in the Cloud becomes accessible to the government and either by accident or through some sort of fishing expedition, what I would consider to be my private communications are accessible to the government or worse yet, become public. How are we addressing those concerns?

Mr. BAKER. We have to make sure, as I mentioned earlier, that we have clear and understandable laws in place to protect the legitimate privacy expectations of Americans. We absolutely want that to happen. There are a range of different laws today that protect your privacy, so whatever we do, we need to make sure we address all of those sort of holistically, if you will, because different types of data are protected under different regimes and we need to make sure we do this in a smart way. There are a variety of laws that are implicated and we need to closely look at all of those.

Mr. FARENTHOLD. I am out of time. Thank you all very much.

Mr. CHAFFETZ. I will now recognize the gentleman from Idaho, Mr. Labrador, for 5 minutes.

Mr. LABRADOR. Thank you, Mr. Chairman.

As you know, there are private sector organizations that exist today that are working to help private industry help protect against these cyber threats. The estimate is about 80 percent of our cyber threats to security and critical infrastructure is through the private sector. For example, many of the critical infrastructures have organizations within which companies can share threat information and best practices. The government should always be looking to these organizations to assist in the effort to protect the country.

Do you currently work with any private sector organizations to facilitate the threat information sharing and best security practices and if you do, can you tell me which organizations you are working with?

Mr. SCHAFFER. Indeed, the Department of Homeland Security is working with many private sector organizations in an effort to share best practices and to share information about threats and vulnerabilities. We work through the Sector Coordinating Councils under the National Infrastructure Protection Plan; we work with the ISAC organizations, the Information, Security and Analysis Centers for the various sectors, including the financial services sector; the multi-state ISAC which goes to State and local govern-

ments; and the IT ISAC representatives from the communications sector. We work with all of those ISAC organizations.

Not only do we work with them, but we have been working to integrate them into our process on the National Cybersecurity and Communications Integration Center watch floor. We actually have representatives from many of the sectors who are either on or coming onto the floor and will participate in the incident response plan processes to address issues when they occur.

We are working extensively with private sector organizations. We can certainly get you a full list if you would like after the hearing.

Mr. LABRADOR. Anyone else want to add anything to that?

Mr. SCHWARTZ. NIST is designed to work very closely with a range of private sector players, including the standards development organizations and the wide range of other private sector standards setting organizations and take the standards best practices from their side, take the standards best practices from the government side and develop those to do work within the Federal Government and vice versa.

A lot of standards that are developed within the Federal Government are then taken into the private sector and are free and open for them to use as well. We have a strong relationship and we could get you a full list if you like.

Mr. BUTLER. For the Department of Defense, consulting, services and products are heavily engaged with a lot of different security firms with regards to ensuring we have the latest and greatest products installed. HBSS is an example as we kind of worked through the Wikileaks mitigation but continuous efforts working with them on threat mitigation.

Mr. BAKER. A significant amount of information sharing goes on as well with respect to law enforcement agencies, back and forth. Obviously when you have a crime that has occurred, you have information sharing that goes on, but in other forums, law enforcement agencies, the FBI, the Secret Service, are working regularly to make sure this information is shared back and forth.

Mr. LABRADOR. I have one more question. While protecting ourselves from cyber attacks we know is extremely critical, many private industry individuals have witnessed a proliferation of Federal initiatives dedicated to this issue. For example, there are over 25 different working groups or task forces being led by the Federal Government. Is there any analysis being conducted right now that would provide ways to streamline this activity to avoid duplicative spending and minimize the amount of Federal dollars spent?

Mr. SCHAFFER. I think we are continually looking, Congressman, at ways to coordinate our activity and make sure the groups we are working with are focused on different problems and are bringing to the table not duplicative but complementary sets of information. I know within DHS, we have several groups that do have overlapping jurisdiction, if you will, they have some of the same members, but we have them focused on different pieces of the elephant that is the cybersecurity problem. We are working to try to coordinate and make sure we are not introducing a lot of redundancy.

Mr. SCHWARTZ. We haven't been afraid to close down working groups that have outlived their time. Everyone working on this issue has many meetings to go to for many of the different task

forces and the fewer we can have is a benefit. I think there has been leadership in that regard in terms of trying to work through a problem, cut it off and move on when we can do that.

Mr. LABRADOR. Thank you. I yield back.

Mr. CHAFFETZ. The gentleman yields.

I will now recognize the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank the panel for their testimony today.

I want to return to an issue I raised in my opening comments. Some members have objected to updating our Federal cyber readiness due to potentially large, upfront costs. Undoubtedly, these efforts will save billions of dollars in efficiencies while providing long, overdue cyber protections and integrity to our Federal networks.

This question would be more appropriate for an entity with a top line view of our cyber efforts across all government agencies such as the cyber director that I have proposed. However, since the administration's current cyber coordinator lacks this authority and as DHS is taking on the operational lead on these efforts, I am going to pose the first question to Mr. Schaffer and then to the rest of the panel.

Mr. Schaffer, what is your assessment of the costs required to carry out the administration's plans to move to an IT infrastructure based on continuous monitoring and automated reporting that was proposed by the administration in its legislative proposal, what efforts have already been implemented, and what are your projected estimates on cost savings and efficiencies and security as a result of these efforts?

Mr. SCHAFFER. I think the key to the FISMA reform proposal is that we recognize much of the work, effort and spending that is done today to meet the FISMA requirements that are really compliance oriented, check the box kind of exercises with an annual report can be repurposed in a way that allows us to actually buy down risk through the continuous monitoring and other solutions being proposed.

The work that we are doing with the departments and agencies on a general basis to improve cyber security across the board can also be done in a way that will get us to better FISMA compliance.

I can't give you a dollar figure with respect to how much it will cost, but I can tell you that we believe over the long run, if this is done and security is improved as dramatically as we think it can be, the expense associated with all the work we do to chase the problems and address all the intrusion activity that is happening will be reduced. Net, I think we will have a positive result over the long run.

Once we start building security into everything we are doing, there is consistent data that suggests building it in is much cheaper than bolting it on.

Mr. LANGEVIN. The other parts of my question, what efforts have already been implemented and what are your projected cost savings on the efficiencies and security as a result of the updates?

Mr. SCHAFFER. We are certainly happy to work with you to think about how to score this. I don't have any numbers that I can present today with respect to estimates of what the actual savings

would be. Again, we know this is the beginning of a conversation and a proposal and expect the final result may or may not look exactly the way we are now, but we certainly want to work with you and the committee as we think about what the cost estimates will be.

Mr. LANGEVIN. Let me move on to another question. I have noticed that one element left out of the legislative proposal was a strengthened White House office with budgetary authority and Senate confirmation. This is something I feel strongly about. In fact, just last year, the White House moved further away from this model by moving OMB's oversight for the Federal security to DHS.

While DHS clearly has the operational lead for protecting the .gov network, what authority do they have to oversee agency budgets and actually compel these important technical challenges actually be addressed? The various departments and agencies, their mission, looking at State or Commerce, isn't necessarily the security of our .gov network. How do we actually compel compliance? OMB could do it but does DHS have that sufficient authority because I really question that. Also, I would like to know why wasn't a strengthened White House office considered?

Mr. SCHAFFER. In the delegation of authority from OMB to DHS to undertake the work we are now doing on FISMA, OMB retained the budget authority to effectively be the entity that enforces those requirements from a budgetary perspective. DHS, as you pointed out, has the operational responsibility.

The legislative proposal would consolidate the oversight responsibility with the operational responsibility that we have and move things in the direction where we would be given the authority to direct departments and agencies to take action to improve their security and deploy appropriate protection.

With respect to today, you have a dual arrangement where DHS has the operational responsibility and OMB has the budget responsibility. That is the way it would line out I think today.

Mr. LANGEVIN. I know my time has expired, but for the record, I would like to get an answer to the question of why a strengthened White House office wasn't considered?

I yield back.

Mr. CHAFFETZ. I now recognize myself for 5 minutes.

Mr. Schaffer, according to press reports, the U.S. Chamber of Commerce has rejected the legislative proposal as "regulatory overreach." We found an internal Chamber document that revealed that the Chamber believed "layering new regulations on critical infrastructure will harm public/private partnerships, cost industry substantial sums and not necessarily improve national security."

Their general concern is that it is overly broad. How do you respond to that and how involved is the Chamber in these types of discussions?

Mr. SCHAFFER. I believe this proposal is carefully crafted to give industry a strong voice in designing the solutions, so it is hard to understand the suggestion that it will be overly expensive or over reaching when in fact, industry will have an opportunity to say what the threats are that need to be mitigated, what the framework should be in order to address those risks and then develop their own plans in order to meet those frameworks.

Mr. CHAFFETZ. Part of this proposal calls for Homeland Security to authorized to publicly name critical infrastructure providers whose plans you deem to be inadequate and then publish those. How is that going to help protect them?

Mr. SCHAFFER. The transparency at the end of the day will engage market forces, we believe, in order to drive toward better results.

Mr. CHAFFETZ. You are going to tell the world, here are the weakest of the weak. Is that what your plan is?

Mr. SCHAFFER. The proposal would provide summaries of the plans and summaries of the evaluations. It is not as if all of these entities aren't under attack today and if they are weak, in fact, the adversaries are taking advantage of them. The proposal here is to make sure that not just the adversaries know they are weak, but in fact, the public knows and the markets can take appropriate action.

Mr. CHAFFETZ. So which of these companies would be required to report to the SEC, for instance, and have their plan certified as sufficient? How does that work?

Mr. SCHAFFER. Those who are already subject to SEC reporting requirements would be required to include this information in that reporting. The proposal doesn't include any suggestion that others would be required to come into that kind of reporting.

Mr. CHAFFETZ. I have a lot more questions about that but given the time, I want to go to one other quick subject. Let us focus with Mr. Butler and Mr. Baker here.

Obviously a lot of these concerns come from overseas players who are a little bit outside of our reach but increasing penalties, how do we highlight these concerns? If someone walked into a computer and physically blew it up, it would be national news, a big deal. If someone comes in through the back door electronically and is blowing up, destroying or stealing information, nothing seems to happen, nobody seems to know. How do we expose this and what kind of penalties can we possibly put in place?

Mr. BAKER. The issue is making sure we have the penalties in place that we then can try to enforce. The enforcement part, I agree with you is a separate question and a separate thing we need to deal with. We deal with that in a variety of different ways, principally through appropriations to make sure we have enough people who are skilled in this area to go out and do this around the world.

Mr. CHAFFETZ. How does that work on the international stage when you have someone who is in some other country doing this?

Mr. BAKER. Internationally, the FBI and the U.S. Secret Service are engaged every day in working with international partners to bring these kinds of people to justice.

Mr. CHAFFETZ. How many of them are actual state actors? You have some kid in a van down by the river, I am sure, in some other country doing this stuff, but you also have concerted efforts from state sponsors. What are we doing about that?

Mr. BAKER. On the state sponsors, I think I will defer to DOD on that one.

Mr. BUTLER. In May, the White House issued the International Cyberspace Strategy which beings to lay out principles and norms that will guide our efforts as we try to engage on this problem you

highlighted. One of the ideas is to work with nations to determine what is going on inside their sovereign territory and like-minded folks getting together to figure out what we need to do so we can not only share information.

Mr. CHAFFETZ. My specific question is when you know it is an actual country, a state, what are we doing about that? If someone were to fire upon us, we would be outraged, but if they seem to do it as a cyber attack, it seems to be quietly pushed under the rug because we don't want to be embarrassed.

Mr. BUTLER. Again, I will go back to the International Cyberspace Strategy for a moment. We say in that document that as we look at cyber incidents and we deem potentially this is something malicious and as we work through attribution, we reserve the right to respond, and that is through a variety of means. Those include law enforcement means, diplomatic means and what have you. We are just at the beginning of now moving from that declaratory position to now considering policy priorities.

Mr. CHAFFETZ. Obviously we are going to have to explore this in greater detail. We know it is happening on all levels in all forms and it is one of the biggest threats to the United States of America.

If there aren't any other questions from any other Members? Yes, the ranking member.

Mr. CUMMINGS. I just want to thank you all but I also want to remind you, piggybacking on what Mr. Chaffetz just said, 9/11 should be seared in all our memories and I know it is, but the terrorists were trying to send a message, several messages and one of them was disruption of our way of life.

When you think about terrorists and now that we have killed Osama Bin Laden, trying to figure out ways to bring harm to the United States, and everyone says how are they going to do it next, somebody can actually sit a computer and do all kinds of harm. I can hear from you we are dealing with this in the words of the President, with the urgency of now, because it is extremely urgent. I hope we will move this along as rapidly as possible.

Again, I want to thank you.

Mr. CHAFFETZ. I also want to echo and thank you for your work, your dedication and commitment. It is a very difficult and challenging question. It is something incredibly nimble and continues to evolve and change. There is no end to the creativity of terrorists and others who wish harm to the United States of America. We don't want to have another major, major incident, someday we wake up and some major portion of our infrastructure, whether private or public. This has to have a lot more attention placed upon it. We certainly don't want to have the kind of incident that we would all regret knowing we could do everything we can to help prevent it.

At the same time, I think we also need to recognize we need to preserve people's individual liberties, need to make we don't overstep and overreach into what private companies are doing, and finding that right balance will be one of the challenges for this Congress and in the future Congresses as well, but we will do so, I hope, in a very bipartisan way.

We thank you for your expertise. We thank you for being here today.

The committee stands adjourned.
[Whereupon, at 11:05 a.m., the committee was adjourned.]
[The prepared statement of Hon. Gerald E. Connolly follows:]

Statement of Congressman Gerald E. Connolly
Committee on Oversight and Government Reform
July 7th, 2011

Cybersecurity should be one of the top priorities for this committee. During the last session, we reported the FISMA Amendments Act, which would have provided a much-needed update to the Federal Information Security Management Act as part of the National Defense Authorization Act, but unfortunately the Senate did not include analogous language. I appreciate the committee's interest in developing a FISMA update and other cybersecurity language. We urgently need reform because the cyber threat is growing. Cyber attacks against federal agencies increased 40% last year, growing from 30,000 to 41,776. Since 2007, the number of cyberattacks has grown 300%. In addition Congress has been the subject of tens of thousands of cyberattacks, including a high profile attack on the Senate's website in June.

The Senate and the House are undertaking different approaches to a comprehensive cybersecurity update. Senate committee Chairmen and Ranking members have submitted a unified cybersecurity proposal to Majority Leader Reid, whereas individual House committees are developing individual cybersecurity bills within each committee's jurisdiction. Whether Congress ends up passing a single cybersecurity omnibus or several smaller bills, the important thing is to get the policy right and make some progress prior to the end of this Congressional session.

President Obama has submitted a comprehensive legislative proposal to update cybersecurity standards. It would establish national data breach reporting standards, improve coordination between DHS and state and local governments, strengthen infrastructure such as the electric grid, improve federal information management, improve agencies' ability to hire skilled cybersecurity personnel, and use cloud computing to improve cybersecurity. The administration deserves credit for developing a detailed cybersecurity proposal, and I appreciate the opportunity to hear more about the plan from the administration witnesses today. As we learned from hearings before this committee during the last session, cybersecurity reform must include a change from compliance to performance based measurements of cybersecurity performance. Unfortunately, while agencies have done a reasonably good job conducting cybersecurity trainings those sessions have not translated into reduced numbers of successful cyberattacks. The administration has already been taking steps to improve cybersecurity. For example, the technology advocacy organization TechAmerica issued a press release praising the administration's smart grid plan as a "major step forward." NIST and other agencies are working to implement the smart grid plan, partially with $20 billion in smart grid funding allocated under the Recovery Act.

Improving cybersecurity is a challenge because of rapidly changing technology and many stakeholders who must all be at the table. Information of the federal government and our constituents cannot be secure without a partnership with private sector providers of technology infrastructure, so it will be critical that we continue to develop cybersecurity plans in partnership with the private sector. In addition, we will have to implement personnel policies that allow the federal government to recruit and retain cybersecurity personnel who can keep up with rapidly changing technologies. The lead division of DHS charged with promoting cybersecurity only has 70 federal employees and 80 support contractors, which is probably insufficient. Shortchanging the federal workforce ultimately puts our citizens and private businesses at risk because federal employees are on the front lines of cybersecurity reform. Thank you again to the witnesses for participating in this important effort.